João Artur Marcelino Pacheco

Master of Science

Performance Evaluation of Class A LoRa Communications

Dissertação para obtenção do Grau de Mestre em

Engenharia Electrotécnica e de Computadores

Orientador: Rodolfo Alexandre Duarte Oliveira, Prof. Auxiliar c/ Agregação,
NOVA University of Lisbon

Júri

Presidente:	Doutor João Carlos da Palma Goes
Arguente:	Doutor Francisco António Taveira Branco Nunes Monteiro
Vogal:	Doutor Rodolfo Alexandre Duarte Oliveira

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Março, 2019

Performance Evaluation of Class A LoRa Communications

Este documento foi gerado utilizando o processador (pdf)LaTeX, com base no template "novathesis" [1] desenvolvido no Dep. Informática da FCT-NOVA [2].
[1] https://github.com/joaomlourenco/novathesis [2] http://www.di.fct.unl.pt

To my Mother and Father

Acknowledgements

First and foremost I would like to express my deepest gratitude to my supervisor, Professor Rodolfo Oliveira, whose guidance and deep knowledge in the subject matter were crucial in the development of this work. As my teacher and mentor he has given more me useful guidance, insightful comments, and considerable encouragements than I could ever give him credit for here. I would like to show my gratitude to António Furtado who was always willing to help and guide me at any given time. His previous work was an essential part of this thesis.

This work would not be possible without the financial support provided by the Projects InfoCent-IoT (POCI-01-0145-FEDER-030433) and CoSHARE (LISBOA-01-0145-FEDER-0307095 - PTDC/EEI-TEL/30709/2017), funded by Fundo Europeu de Desenvolvimento Regional (FEDER), through Programa Operacional Regional LISBOA (LISBOA2020), and by national funds, through Fundação para a Ciência e Tecnologia (FCT).

Last but not least, i would like to show my unending thankfulness to my family and friends, especially to my parents and sister, who always stood by my side. Their love and guidance are with me in whatever I pursue. I can not express in words how thankful I am for all the opportunities they provided me.

Abstract

Recently, Low Power Wide Area Networks (LPWANs) have attracted a great interest due to the need of connecting more and more devices to the so-called Internet of Things (IoT). This thesis explores LoRa's suitability and performance within this paradigm, through a theoretical approach as well as through practical data acquired in multiple field campaigns. First, a performance evaluation model of LoRa class A devices is proposed. The model is meant to characterize the performance of LoRa's Uplink communications where both physical layer (PHY) and medium access control (MAC) are taken into account. By admitting a uniform spatial distribution of the devices, the performance characterization of the PHY-layer is studied through the derivation of the probability of successfully decoding multiple frames that were transmitted with the same spreading factor and at the same time. The MAC performance is evaluated by admitting that the inter-arrival time of the frames generated by each LoRa device is exponentially distributed. A typical LoRaWAN operating scenario is considered, where the transmissions of LoRa Class A devices suffer path-loss, shadowing and Rayleigh fading. Numerical results obtained with the modeling methodology are compared with simulation results, and the validation of the proposed model is discussed for different levels of traffic load and PHY-layer conditions. Due to the possibility of capturing multiple frames simultaneously, the maximum achievable performance of the PHY/MAC LoRa scheme according to the signal-to-interference-plus-noise ratio (SINR) is considered. The contribution of this model is primarily focused on studying the average number of successfully received LoRa frames, which establishes a performance upper bound due to the optimal capture condition considered in the PHY-layer. In the second stage of this work a practical LoRa point-to-point network was deployed to characterize LoRa's performance in a practical way. Performance was assessed through data collected in the course of several experiments, positioning the transmitter in diverse locations and environments. This work reports statistics of the received packets and different metrics gathered from the physical-layer.

Keywords: LoRa Networks, PHY/MAC Modeling, Performance Evaluation.

Resumo

No passado recente, a necessidade de conectar cada mais dispositivos à chamada Internet das Coisas, despertou um interesse por redes de baixa potência e longa distância (LPWANs). Esta dissertação explora a aptidão e desempenho da tecnologia LPWAN LoRa, tanto através de uma abordagem teórica, bem como da análise de dados práticos recolhidos em várias campanhas. Primeiramente é proposto um modelo de avaliação de desempenho de dispositivos LoRa de classe A. O modelo foi desenvolvido com o propósito de caracterizar o desempenho do Uplink LoRa, considerando a camada física bem como a camada de controlo de acesso ao meio. Admitindo que os dispositivos estão uniformemente espacialmente distribuídos, a caracterização do desempenho da camada PHY é estudada através da derivação da probabilidade de descodificar com sucesso vários pacotes enviados em simultâneo e usando o mesmo fator de espalhamento. A análise do desempenho da camada MAC é realizada supondo que o tempo entre pacotes é exponencialmente distribuído. É considerado um cenário típico de operação LoRaWAN, onde os sinais transmitidos pelos dispositivos LoRa classe A são afetados por atenuação, zonas de sombra e desvanecimento de Rayleigh. Os resultados numéricos obtidos através da metodologia exposta no modelo são comparados com resultados simulados, ademais, a validação do modelo proposto é discutida segundo diferentes níveis de carga na rede e condições na camada PHY. Devido à possibilidade de multi-captura simultânea, os resultados representam o máximo de desempenho alcançável num esquema PHY/MAC LoRa em relação a um rácio entre sinal e ruindo mais interferência (SINR). A principal contribuição deste modelo reside no estudo do número médio de pacotes LoRa recebidos com sucesso, pelo que considerando a condição óptima de captura definida na camada PHY, representa um limite superior de desempenho. Na segunda parte deste trabalho, é operacionalizada uma rede ponto a ponto de forma a caracterizar na prática o desempenho das comunicações LoRa. O desempenho é avaliado através de dados recolhidos no curso de várias experiências, no qual o transmissor foi posicionado em diversos locais e ambientes. São reportados os dados recolhidos, bem como estatísticas dos pacotes recebidos e diferentes métricas da camada física e de controlo de acesso ao meio.

Palavras-chave: Redes LoRa, Modelação PHY/MAC, Avaliação de Desempenho.

Contents

List of Figures

List of Tables

Glossary

Backhaul	The intermediate links between the backbone network and its smaller sub-networks.
Chip	Frequency jump that determine how the data is encoded onto the chirps.
Chirp	A sweep signal, i.e a signal whose frequency changes at a fixed rate, it constantly increases (up-chirp) or decreases (down-chirp).
Hop	Each hop represents a portion o the path between a source and destination.
Link budget	An accounting of all the gains and losses between a transmitter and a receiver.
Noise floor	The resulting signal from the sum of all unwanted interferences and noise sources.
Sensitivity	The minimum magnitude of an input signal required, so that it can be successfully received.
Symbol	A representation of one or more bits of data.
Throughput	Data transfer rate, the quantity of data transfered between two distinct entities or the amount of computed data in a given time interval.

Acronyms

3GPP	Third Generation Partnership Project.
ABP	Activation by Personalization.
ACID	Atomicity, Consistency, Isolation and Durability.
ADR	Adaptive Data Rate.
AES	Advanced Encryption Standard.
AGNES	Agglomerative Nesting.
AMQP	Advanced Message Queuing Protocol.
API	Application Programing Interface.
BD	Big Data.
BI	Business Intelligence.
BPSK	Binary Phase Shift Keying.
BS	Base Station.
CAP	Consistency, Availability and Partitioning.
CEPT	European Conference of Postal and Telecommunications Administrations.
CIoT	Cellular Internet of Things.
CLARANS	Clustering Large Applications based on RANdomized Search.
CoAP	Constrained Application Protocol.
CoRE	Constrained RESTful Environments.
CPS	Cyber Physical System.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Check.
CRUD	Create Read Update Delete.
CSS	Chirp Spread Spectrum.
CVO	Composite Virtual Object.
CVOL	Composite Virtual Object Layer.

DIAT	Distributed Internet-like Architecture for Things.
DL	Downlink.
DNS-SD	Domain Name System - Service Discovery.
DS	Direct Sequence.
DSL	Digital Subscriber Line.
DSSS	Direct Sequence Spread Spectrum.
DTLS	Datagram Transport Layer Security.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number.
ED	End Device.
ERC	European Radio-communications Committee.
ERP	Effective Radiated Power.
ETSI	European Telecommunications Standards Institute.
FEC	Forward Error Correction.
FH	Frequency Hopping.
FHDS	Frequency Hopping Direct Sequence Hybrid.
GSM	Global System for Mobile Communications.
HDFS	Hadoop Distributed File System.
HTTP	Hypertext Transfer Protocol.
IaaS	Infrastructure as a System.
IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force.
iid	independent and identically distributed.
IoT	Internet of Things.
IPSec	Internet Protocol Security.
ISM	Industrial Scientific and Medical.
IT	Information Technology.
KNN	K-Nearest Neighbor.
LBT	Listen Before Talk.
LHC	Large Hadron Collider.

LoRa	Long Range.
LPWAN	Low Power Wide Area Network.
LTE	Long-term Evolution.
M2M	Machine to Machine.
MAC	Medium Access Control.
MIC	Message Integrity Code.
MQTT	Message Queuing Telemetry Transport.
NB-IoT	Narrow Band-Internet of Things.
NFC	Near Field Communication.
NS	Network Server.
OFDMA	Orthogonal Frequency Division Multiple Access.
OTAA	Over-The-Air-Activation.
PaaS	Platform as a System.
PAM	Partitioning Around Medoids.
PDF	Power Density Function.
PDP	Policy Decision Point.
PEP	Policy Enforcement Point.
PER	Packet Error Rate.
PM	Policy Manager.
PR	Policy Repository.
PSD	Power Spectral Density.
QoS	Quality of Service.
QPSK	Quadrature Phase Shift Keying.
RB	Resource Block.
REST	Representational State Transfer.
RFID	Radio-Frequency IDentification.
RFU	Reserved for Future Use.
RSSI	Received Signal Strength Indicator.
RV	Random Variable.
SaaS	Software as a System.

SASL	Simple Authentication and Security Layer.
SC-FDMA	Single Carrier - Frequency Division Multiple Access.
SCTP	Stream Control Transmission Protocol.
SF	Spreading Factor.
SGS	Semantic Gateway as Service.
SINR	Signal to Interference plus Noise Ratio.
SL	Service Layer.
SM	Service Management.
SNR	Signal to Noise Ratio.
SOA	Service Oriented Architecture.
SQL	Structured Querying Language.
SSL	Secure Sockets Layer.
SSOA	Semantic Service Oriented Architecture.
SVM	Support Vector Machine.
TCP	Transmission Control Protocol.
TLS	Transport Layer Security.
UDP	User Datagram Protocol.
UL	Uplink.
UNB	Ultra Narrow Band.
URI	Uniform Resource Identifier.
VO	Virtual Object.
VOL	Virtual Object Layer.
WAN	Wide Area Network.
WoT	Web of Things.
WSN	Wireless Sensor Network.
WWW	World Wide Web.

CHAPTER 1

Introduction

1.1 Introduction

For quite some time, the Cyber Physical System (CPS) concept has been a staple technology in automated industries. CPSs consist of an amalgamation of physical entities and computational elements intertwined such that their components are able to interact with each other, adapt and a react accordingly to their environment. This requiring increasing autonomy, adaptability and reliability.

With technological advances the Internet of Things (IoT) paradigm emerged and expanded the concept of connection and communication of virtual and physical entities to the Internet. The endless possibilities of applications, combined with cheap and readily available hardware and software IoT solutions, allowed IoT devices to be spread over all sorts of industrial and commercial sectors. Currently, the number of operational IoT systems is steadily increasing by the day. Naturally it is an highly researched theme and with new solutions constantly being presented, Internet of Things is quickly turning into one of the fastest growing global markets.

1.2 Motivation

Internet of Things is still a relatively recent concept, but its potential is too high. By improving the connectivity capabilities between computational and physical devices, this paradigm extended Internet connectivity from typical devices (laptops, smart phones, etc.) to everyday objects. This opened the doors to an extensive amount of applications outside the industrial and manufacturing environment. IoT technology is being used from small scale scenarios like smart homes and farms to energy management, transportation or even

metropolitan scale deployments.

IoT greatly enhanced data gathering mechanisms, thus enabling researchers to rapidly gather large amounts of information and decreasing the time necessary to ascertain meaningful conclusions like hidden correlations among a system, behavioral patterns, and social trends. Despite of this, the IoT arena is still characterized by a lack of standardization, making interoperability of devices a bigger challenge. Researchers are actively making efforts towards a future, where devices can be seamlessly integrated into a network and provide ubiquitous computing. LoRa is one of the most prominent technologies for long range connectivity in IoT sytems. A such, this work tries to answer two main questions. First, how would the protocol perform if the gateway had the capacity to simultaneously decode multiple frames, without any additional costs on the end devices. Secondly, what can be expected, performance wise, from the currently available LoRa devices.

1.3 Objectives

The objectives to be achieved in this dissertation are as follows:

O1. In a first step it is required to understand the fundamentals of LoRa's PHY and MAC layer. The goal is to identify LoRa's literature and understand its design and operation to identify and filter important information to be used in this work;

O2. Given the importance of LoRa networks, this work aims to quantify the gain of performance when the gateway is capable of decoding multiple packets at the same time (instead of decoding at most one). This is the main goal of this work, which encompasses the design of a theoretical framework to model the physical and the MAC layers in a cross-layered design. The performance assessment is based on the comparison of the numerical results (obtained with the theoretical model) with simulation results;

O3. This objective targets the performance evaluation of a practical LoRa system. This includes the acquisition of LoRa devices, the study of their programming interfaces, the design of realistic and diversified experimental scenarios, and at a final phase the gathering of LoRa communications' statistics and their statistical analysis.

1.4 Contributions

Regarding the contributions of this work, we list the following ones:

C1. A brief overview of IoT and LoRa networks was written, which supports the fundamentals to study LoRa networks;

C2. A theoretical model is proposed to compute the upper bound of LoRa's performance when the gateway is capable of decoding multiple packets at the same instant. The

theoretical model was compared with simulated results to evaluate its accuracy. This contribution was also reported in a conference paper that is currently under review in a Q1 Scimago conference (submitted to the 15th International Wireless Communications and Mobile Computing Conference, Tanger, Marrocos (IWCMC 2019) - the paper is copied in Annex I);

C3. A comprehensive study of the hardware acquired to achieve the objective O3 in order to design and operationalize multiple tests to be conducted at different scenarios. This contribution has to do with the practical data obtained with LoRa devices, which is discussed in this dissertation and will be worked to prepare a technical paper in the near future.

1.5 Outline

This work aims to explore currently available Internet of things technologies and architectures as well as disclose LoRa's suitability in this context.

Chapter 2 presents a brief explanation of the IoT paradigm, followed by a general description of the some technologies and techniques that support it.

Chapter 3 is aligned with the objective O1. A detailed explanation of LoRa's protocol is provided. This involves the specification of techniques employed by LoRa, such as the methods used to decode and or recover data from a packet that suffered transmission errors, the coding scheme, the methodology of increasing signals' resilience to noise, and its effect on the time on air of a packet. LoRaWAN's MAC layer is also specified. It encompasses a clarification on the structure of both uplink and downlink messages, the types of messages available and the protocols intricacies, such as the joint procedures between end devices and the gateway when the former attempts to join the network. Additionally, Chapter 2 contains a brief report on the transmission limitations imposed by the regulatory bodies.

Chapter 4 describes the work to address the objective O2. It proposes a theoretical model to characterize LoRa's uplink performance. The proposed model is be divided into two stages: model description, and performance evaluation. The former provides a detailed description of the considered network scenario, PHY layer performance characterization, MAC layer access probability, as well as the performance characterization of the joint PHY and MAC layers. The network scenario includes the network structure, nodes' spatial distribution and propagation conditions, namely the path loss, the modeling of shadowing and Rayleigh fading along with the modeling of their composite effect. The PHY layer section specifies how the performance characterization is accomplished through the probability of successfully decoding a frame. Regarding the MAC layer, the access behaviour is described as a Poisson process considering the network load. The joint PHY/MAC performance contains the process used to describe the success probability when accounting for both the MAC and PHY layers. The contribution of this model is primarily focused on studying the average number of successfully received LoRa frames, which

establishes a performance upper bound due to the optimal capture condition considered in the PHY-layer.

Chapter 5 describes the practical assessment tests and results aligned with objective O3. Several tests are described considering that the transmitter is placed at different locations to evaluate LoRa's link performance in different propagation environments. The data gathered in real time is then statistically treated to determine the achieved performance.

Finally, Chapter 6 presents final remarks and discusses different paths to extend this work in future efforts.

CHAPTER 2

State of the Art

2.1 Cyber Physical Systems

Cyber Physical Systems (CPSs) represent systems where the computation process and physical data are intrinsic, being characterized as a boundless network of devices, computational resources, applications, and services interconnected amongst themselves. CPSs are usually managed through the use of a broad spectrum of sensors, actuators and communication topologies. This technology allows to hypothesize a future where a system can monitor physical information, while simultaneously analyzing such information in its cybernetic layer. This grants the ability to react accordingly and preferably in real time. All in all, despite the advantages this trend brings, a new set of problems arise. A system abiding by this specifications inherently consumes and generates huge amounts of data, which can possibly be problematic due to limitations akin with current hardware processing power and available storing space. Fortunately, with the exponential growth of Internet of Things (IoT) systems and Cloud computing, is possible to outline these adversities.

Considering all the characteristics previously discussed, a CPS has three main requisites to fulfill:

1. Support an intense rate of computation;
2. Store and analyze extensive influxes of information;
3. Enable continuous access to all stored information, through the means of a graphical user interface.

All these three demands can be met through a blend of cloud computing and a wide band connection (IoT) to the system in question. The IoT layer is seen as the mean to enable sensors and actuators integration to the internet. Cloud processing is one of several

methods of computation compared in Table 2.1. An alternative to cloud computing is Cluster computing, which is essentially a form of distributed computation. The process is shared by a multiplicity of computers and storing apparatus, interconnected in order to convey to an user the illusion of it being run a single device. Naturally, the processing capabilities are tied to the number of machines that constitute the network. According to the study [60] the capabilities of a system that employs cluster processing is directly proportional to the number of CPUs used, which makes this paradigm quite expensive to operate. Grid computing consists of several computers interconnected in order to complete a task. The key difference is this paradigm reliance on a control software designed to split a complex task into more manageable steps. Each of those subdivisions is then assigned to a set of computers, members of the network. This technology has been implemented in some Wireless Sensor Networks (WSNs), like the solution described in [28], but its use is only expedient in a system whose processes hold a level of complexity such that it as to be distributed amongst different computers. In an environment where the priority is to guarantee the processing of high data influxes, Cloud computing presents itself as a cheaper and easier to implement archetype.

	Cluster Computing	**Grid Computing**	**Cloud Computing**
Loose-coupling	No	Both	Yes
Resource Handling	Centralized	Distributed	Both
Application/ Service Oriented	Application	Both	Service
Hardware	Commodity	Commodity	Mixed
Up Front Cost	Medium	Medium	Low
I/O Performance	Low	Low	Medium
Rapid Elasticity	No	No	Yes

Table 2.1: Overview comparison of computing methods [60].

As a result of the combined low cost and high flexibility, Cloud computing is an important technology when scalability is taken into account.

Clouds solutions and data analytics techniques will be addressed in further detail in Sections 2.6 and 2.8.

2.2 Internet of Things (IoT)

In a nutshell, IoT constitutes the networking structure of a cyber physical system, for information transfer purposes. Its basic principle is to allow autonomous and secure connections to achieve data exchanges between physical world devices and applications, acting as a link that connects the physical and virtual world. As a whole it is a compound of objects, sensors, communication infrastructures, computational and processing units, decision making, and action mechanisms [31].

This concept forces IoT to be capable of connecting a endless number of heterogeneous objects over the Internet, meaning its architecture must be as flexible as it can be. Figure 2.1 displays several adopted models.

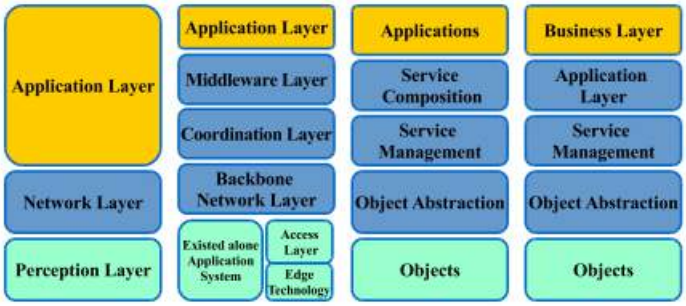


Figure 2.1: IoT layer architectures [4].

The three layers architecture, illustrated in Figure 2.2, is the simplest of all four models. In [76] the purpose of each layer is defined in the following manner. The perception layer is responsible for collecting and capturing data. It should perceive the devices that compose it, virtualize them into heterogeneous objects and feed their information to the upper layer. In a perfect scenario this layer should be capable of integrating every apparatus on the network. The challenge is to make it capable of perceiving and recognizing the maximum number of devices, using the least amount of power, and do that in an economic way. The network layer has the task of enabling long distance exchanges of the information, recalled by the previous layer, and its computation. The computation is usually done in a cloud environment as it is effective and cheap. Lastly, there is the application layer whose main purpose is service discovery and arrangement for communities or clients, where the information collected by the system is shared and treated accordingly. In a system designed to read temperature and humidity levels, this layer is the one that conveys sensors readings to the user, on demand. Given the abundance of networking technologies the exchange of information from the network layer to the application layer can be problematic as there is not a market standard and it is impossible to implement every protocol. Solutions like gateways have been designed to counterbalance this situation, but more or less some sacrifices have to be made, depending on the target application.

The five layer architecture presented in Figure 2.3 is an evolution of the simpler form that adds more abstraction to the IoT model[4]. The perception and application layers remain identical and act as described earlier. The object abstraction layer, also known as transport layer transfers the information collected from the sensors (object perception layer) to the service management layer in a secure manner. Data can be exchanged through a plethora of protocols like NFC, RFID, Bluetooth, ZigBee, etc.. Service Management or Middleware layer stores, analyses, and processes huge chunks of data using technologies such as databases and cloud computing. As the name implies, this layer also associates services to user's requests. The Business layer oversees and manages all the other layers. Quality of service is reinforced at this level through comparison of real and expected layer

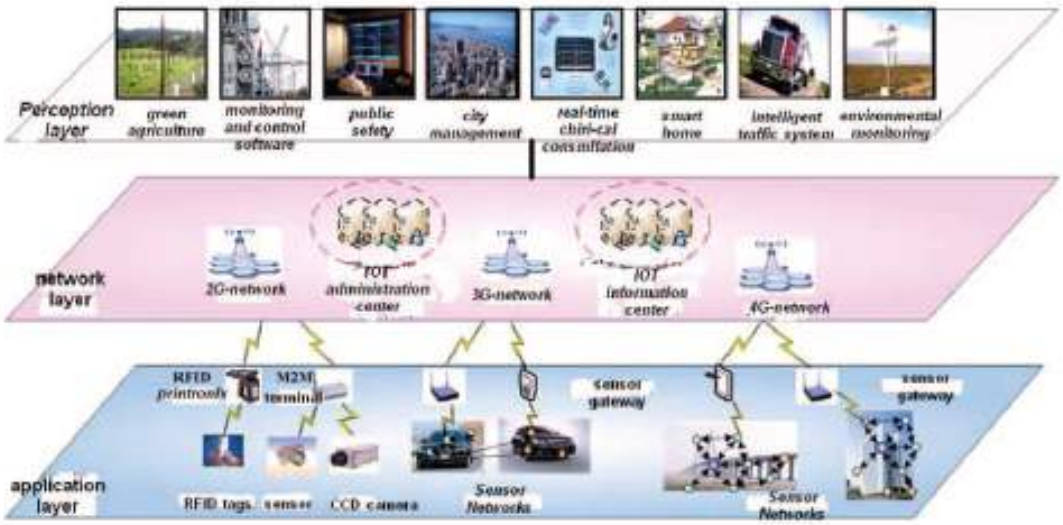


Figure 2.2: IoT three layers architecture [76].

outputs. Additionally, it handles decision making based on big data (BD) analysis and business models strategies like data organization and visual representation (statistical graphs, flowcharts, plots, etc.).

The five layer architecture is able to answer IoTs demands and offers enough flexibility to be tweaked for different applications, resulting in slight variations as illustrated in Figure 2.1, regardless the basics of each layer remains the same and the fundamental functions (identification, sensing, communication, computation, services and semantics) are always present.

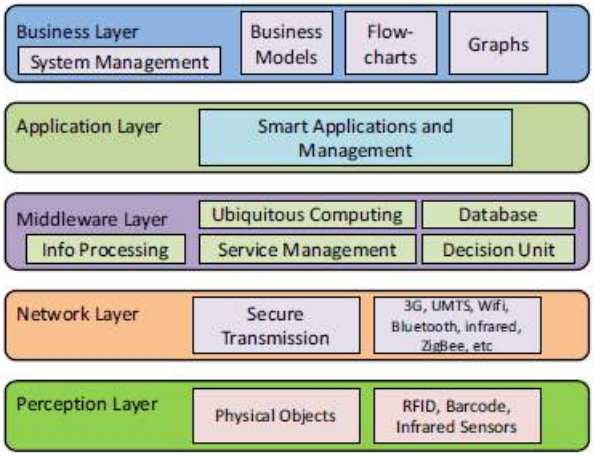


Figure 2.3: IoT five layer architecture [31].

2.3 Heterogeneity and interoperability of information

2.3.1 Gateway

One of the core points of a wireless sensor network is the gateway. It acts as an intermediary between sensors and the Internet, a process called hub-and-spoke model [15]. Translation of protocols for encryption, processing, filtration and maintenance of information exchanged by the system are all integral responsibilities of this element [68]. The absence of a consensus or standard regarding communication between sensors and the system in which they are to be integrated, impose a high level of complexity on the gateway, from a functional stand point. Furthermore the idea of a standard communication protocol is very questionable in an IoT environment, the vast extent of possible applications make it almost impossible to extend a single protocol for all types of applications [43]. All this implies that the heterogeneity of an IoT system requires the ability to establish communication with the biggest array of sensors, and the gateway has to offer support for a substantial number of protocols.

The challenge lays in the fact that despite the abundance of available technologies, none is disposable, because each one has specific features that make them more or less appropriate, depending on the specifics of each application.

Features	**Technologies**			
	RFID	**NFC**	**Zigbee**	**Bluetooth**
Peak distance	3-10 m	10 cm	100 m	10-100 m
Data rate	640 kbps	106-424 kbps	250 kbps	<1 Mbps
Capability	Identifying, Storing, Interacting	Interacting	Secure sharing of data	Sharing, Identifying
Used in	Logistics, Transportation, Retail, Payments	Smart phones, Access control, Contactless payments	Industrial controls, Digital Agriculture	Retail, Healthcare, Transportation

Table 2.2: Comparison of characteristics of transport layer technologies in IoT.

In Table 2.2, adapted from [15], it is possible to observe the different applicabilities of each technology. The authors of [70] reinforce this idea stating that RFID and NFC are very comparable at an application level, although in the context of device-to-device communication, the later manifests an easier and more intuitive to implement. On the other hand the study also points the importance that Zigbee has in the home automation market. It offers consumers unprecedented control and choice in this environment by providing standard interfaces for lighting control, motorization, security, etc... Taking into account that all of these protocols belong to the IoT communication/transport layer and already cause interoperability problems, if all layers of such system are taken in account,

the spectrum of choice possibilities broadens significantly, greatly increasing this issue. For example, according to [4], at the application level, some of the efforts of standardization also include lightweight data protocols, such as the Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Advanced Message Queuing Protocol (AMQP), and others, summarized in Figure 2.4, extracted from [4].

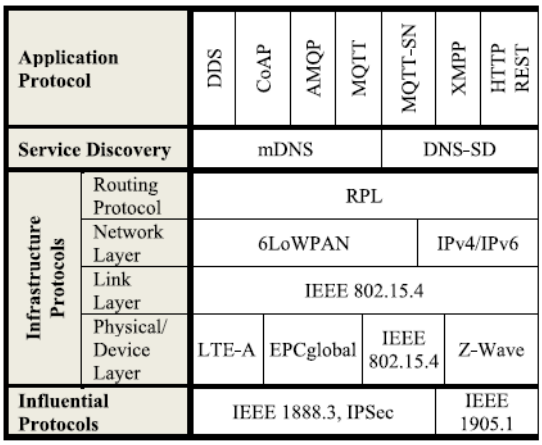


Figure 2.4: Standardizations in the IoT plane.

All these initiatives increase lack of interoperability amongst sensors. In [72] it is mentioned that although the IoT domain is scattered between low powered protocols (ZigBee, Bluethooth) and traditional ones (WiFi, Ethernet), standardization can be achieved by assembling hardware with the required components. In other words, this concept may be implemented through different device configurations including but not limited to a microprocessor equipped with communication modules.

Despite the aforementioned, the compatibility problem is still very relevant regarding the application level.

2.4 Application Protocols

In the last section it was established that the biggest challenge haunting WSNs integration is the broad spectrum of protocols available. For the sake of better understanding this problem it is necessary to recognize the options offered in the marketplace.

Application protocols run over the application layer of an IoT system. This layer is responsible for providing customers their requested services, like getting temperature sensor measurements to a customer owned software, on request. It covers numerous markets such as smart home, smart building, agriculture, transportation, industrial automation and smart healthcare [31], whereby the choice of protocol is determined in accordance with the demands imposed by industry where the system is going to operate.

2.4.1 Web Protocols

It is broadly accepted that due to the energy constraints of a sensor network, the best way to establish communication is with a lightweight message protocol, like those mentioned in the last chapter, claim backed by the wide array of projects employing or acknowledging such technologies [4, 42, 68, 72].

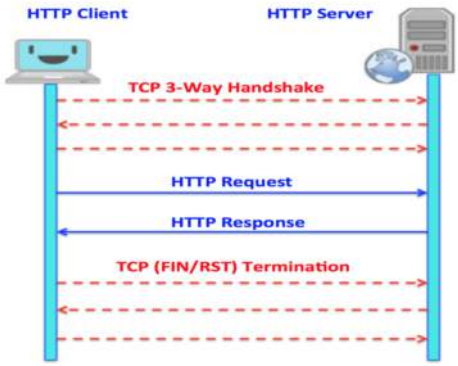


Figure 2.5: HTTP client-server communication [43].

The authors of [43] argued for an alternative solution, instead of relying on traditional IoT protocols, they introduce the concept of Web of Things (WoT). By re-using the existing World Wide Web infrastructure, and web protocols (HTTP) the problem of interoperability can be resolved, although the use of these protocols brings another problem to table, web latency. Time of response can be detrimental to a network that rely on real time action/reaction interactions. Unfortunately, this latency is affected by a number of different factors but mainly on the distance between the client and the server combined with the HTTP and its transport layer protocol (TCP) faults. HTTP incurs several round trips to perform an action, while TCP has a three way handshake system (figure 2.5) required to open a connection for every HTTP round trip combined with the fact that it employs the so called "slow start technique", causing it to not use all the available bandwidth for the first round trips of a connection [42, 43], as an effort to avoid network congestion. Acknowledging this, the authors elaborated a series of tests to determine the viability of this implementation, using two iterations of HTTP, SPDY and HTTP/2, the later being the latest version of the protocol. Four experiments were conducted, analyzing the web latency when both client and server support the SPDY and HTTP/2, when only one supports and finally when neither offers support. The results showed the inadequacy of this implementation, although these versions of the protocol display a decrement of web latency when compared at the server to the first version of HTTP (HTTP/1.1), the client side was void of improvement, leading to the conclusion that only a substantial enhancement can make HTTP a contender in IoT, or equivalent lightweight protocols should take its place. Considering that according to [26] an extensive study of the HTTP/2, even with the improvements over its older counterparts, the protocol is not adequate. The switch to

this version of the protocol is not a simple task and it requires a high number of updates on servers, client browsers, etc. Making it a long process, meaning that it may be a while till HTTP can be considered in the IoT spectrum.

Additionally, in [42], after comparing HTTP, AMPQ, MQTT and CoAP protocols, the authors conclude that "HTTP is a global web standard but mostly not suitable and used in the IoT industry".

2.4.2 Low Power Application Protocols

As the IoT concept renders itself more and more embedded into our lives this breed of messaging protocols has been gaining traction in the industry. Of the plethora of available technologies three stand out as the stronger contenders to become the next the-facto standard: CoAP, MQTT, AMPQ [4, 18, 42, 72].

	CoAP	**MQTT**	**AMQP**
Architecture	Client/Server or Client/Broker	Client/Broker	Client/Server or Client/Broker
Transport	UDP, SCTP	TCP	TCP, SCTP
Messaging	Request/Response	Publish/Subscribe or Request/Response	Publish/Subscribe or Request/Response
User Configurable QoS	Confirmable or Non-Confirmable messages	At-most-once At-least-once Exactly-once	At-most-once At-least-once Once-and-only-once
Network	IPv6/RPL	IPv6/RPL	IPv6/RPL
Adaptation	6LoWPAN	6LoWPAN	6LoWPAN
MAC Address	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4
Physical Address	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4
Security	DTLS IPSec	TLS/SSL	TLS/SSL IPSec SASL

Table 2.3: Overview comparison of low power application protocols.

Message Queuing Telemetry Transport (MQTT) is a messaging protocol that aims at connecting embedded devices and networks with applications and middleware [4]. It was created by IBM initially as a client/server protocol but later morphed into a publish/subscribe protocol [62]. Clients can subscribe to and publish topics to a server that acts as broker. The broker coordinates client subscriptions and grants security to the system by employing client authentication. Sent messages have a QoS tag that dictates how they should be treated:

- **At-most-once** - Messages are sent across the network without the need for acknowledgment. They are delivered at most once or, since these messages are not stored, may not be delivered at all if the client disconnects or the server fails. This setting functions like a fire and forget mechanism;
- **At-least-once** - The message must be delivered at least once, might even be received multiple times until the acknowledgment reaches the sender. A message with this tag must be stored by sender in case it needs to be sent again;
- **Exactly-once** - Similarly to the previous entry, this setting assures the message is delivered to the designated recipient and is saved till confirmation arrives, only it is delivered exactly once. It is the safest mode of transfer but also the slowest because it requires a more sophisticated handshaking and acknowledgment process to avoid message duplication.

This protocol is widely adopted but despite its strengths the fact that it runs over TCP make it unsuitable for some IOT applications, additionally details like the use of text for topic names translate into an overhead increase on the network.

Constrained Application Protocol (CoAP) is a lightweight M2M protocol developed by the IETF CoRE (Constrained RESTful Environments) Working Group, specifically for IoT applications. It is based on REST (REpresentional State Transfer) with a combination of HTTP functionalities, through the use of proxies, and URI [10], making translation to HTTP fairly easy. As HTTP, this protocol utilizes methods such as GET, PUT, DELETE and POST to achieve the four basic operations (CRUD) of persistent storage. Contrary to others it runs over User Datagram Protocol (UDP) with support for multicast addressing (allows group communication). To rectify UDP unreliability, lack of acknowledgment, time outs and retransmission features that ensure sent messages are received, CoAP employs a resource discovery and retransmission mechanism, complete with resource description. CoAP quality of service features still remain somewhat rudimentary as of the four types of messages supported, only two enforce reliability:

- **Non-Confirmable** - Non-Confirmable messages do not need any sort of confirmation from the receiver, essentially message exchange is treated in a fire in forget faction;
- **Confirmable** - The receiver must acknowledge it received the message by exchanging an ACK package with the sender.

ACK messages are used to confirm the arrival of a message, while reset (RST) messages signal communication issues or missing packages. Since it cannot rely on SSL and TLS (available with TCP/IP), CoAP uses Datagram Transport Layer Security (DTLS) to provide secure message exchanges. Arguably this protocol handles resource discovery more effectively than its TCP based counterparts. Traditional TCP/IP networks use DNS-SD that is primarily used to discover services provided by software, whereas IoT carries a much wider spectrum, making an URI based approach an auspicious alternative [63].

Advanced Message Queuing Protocol (AMQP) was developed by John O'Hara at JPMorgan Chase [42]. It supports a request/response (point to point communication) as well as a publish/subscribe architecture. It has five components, broker/server, consumer, message queue, publisher/producer and exchange [37]. The publisher or producer is an application tasked with assembling and sending messages to an exchange on a server. An exchange represents a matching and routing engine that feeds messages from publishers to a message queue inside the server. The broker or server is an intermediary between consumers and publishers, that hosts messages queues and exchanges. Message queues are data structures independent amongst themselves, that sequentially store and deliver messages to the consumer who declared the aforementioned message queque. Finally, a consumer is an application that declares one or more message queues on the server. In short, consumers are clients that by requesting a service declare a message queue on the broker, while publishers are the service providers who send messages to those queues through exchanges. AMQP quality of service properties are identical to MQTT both in behavior and semantics [18]. The security gain in this protocol can be aided by an external security layer running TLS for data encryption or by the use of the Simple Authentication Security Layer (SASL), that is an IETF Standard Track protocol, to negotiate authentication.

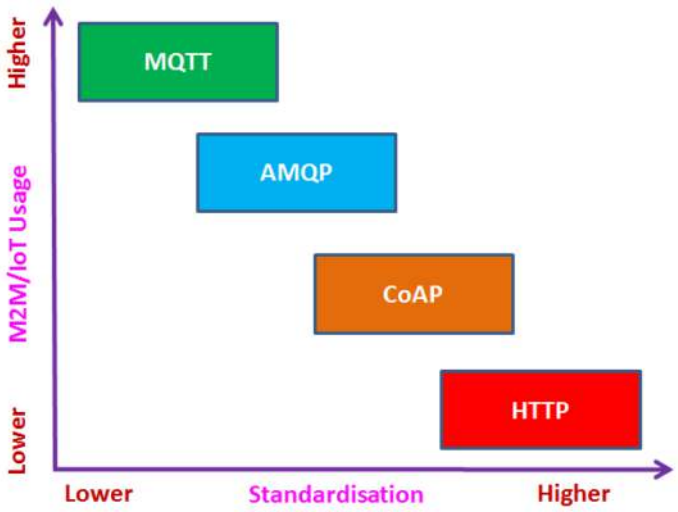


Figure 2.6: M2M protocols usage versus standardization (adapted from [42]).

As illustrated in Figure 2.6, MQTT is an emerging de facto IoT protocol, adopted by companies such as IBM, Facebook, Cisco, etc. Although it stands as the prominent one, MQTT specifications are not sufficient to satisfy all the market needs. AMQP as been used in some of the worlds most impressive programs like Oceanography monitoring of the Mid-Atlantic Ridge and Nebula Cloud Computing by NASA [42]. CoAP has earned the support of industry giants Cisco and open source projects like IoTivity. Despite MQTT popularity, all these examples constitute viable options, the right one is simply the most adequate for the job, dictated by factors like power consumption, resource requirement, quality of service, bandwidth, message size, etc. In fact, in a scenario where packet loss

rate is low, MQTT is able to send messages faster than CoAP, which in turn outperforms the former in the opposite scenario [4]. If reliability is a top priority, MQTT offers an hefty array of reliability and congestion control mechanisms compared to CoAP. In contrast, CoAP is sturdier regarding interoperability due to message fragmentation capabilities borrowed from UDP, that facilitates efficient transmission of large messages in constrained networks resulting in an easier integration between devices and wireless sensor networks [14]. Furthermore, in some instances the strengths and faults of each protocol can became negligible. The aforementioned advantages of MQTT reliability are more prevalent in high data transmission applications and reliability differences decrease otherwise.

2.5 Network Layer Specifications

2.5.1 Low Power Wide Area Network

A Wide Area Network (WAN) spans a large geographical area and it is designed to allow long range wireless or wired communications between devices [71, pp.23-27]. Naturally, Low Power Wide Area Networks (LPWANs) are an adaptation of the WAN concept, developed to enable communication amongst devices which require low power and efficient management of battery life, namely M2M and IoT networks that operate at a lower cost with greater power efficiency than traditional mobile networks (2G, 3G and 4G are far more demanding energy wise). While technologies like RFID, Bluethooth and WIFI excel in a variety of IoT systems, their range limitations depicted in Table 2.2 make them unsuitable for any IoT system designed to operate beyond the limits of a building. Using a LPWAN technology grants commercial and industrial settings the ability to implement IoT systems with a range of kilometers, battery lives up to ten years at a low cost, and enough flexibility to allow easy expansion [74]. The ranges can vary, approximately, from ten to forty kilometers in rural areas and one to five kilometers in urban environments [38], depending on the roll of physical phenomenons like reflection, scattering and shadowing effects have on the transmitted radio waves [74]. Essentially, settings where those effects manifest themselves in high rates are more susceptible to packet losses.

Presently, LPWANs are networks composed by end devices (ED) connected to base stations (BS), arranged is a star formation (star-topology network). In these networks communication is established between ED and a BS, only in rare exceptions end devices are able to transmits data directly amongst themselves. Base stations are connected to a central server via a backbone IP based link and transmit data over a specific band, dependent on the specification used as well as frequency regulations imposed by its physical location [39]. End devices are free to transmit data whenever unless instructed otherwise by a base station.

With decreased energy requirements, longer range than other IEEE 802.15.4-based specifications and lower costs than regular cellular technologies this rather new term, nonexistent as recently as 2013 [66], became one of the fastest growing concepts in IoT

and spread to both licensed and unlicensed frequency bandwidths. However, as illustrated in Figure 2.7, there is a major trade-off in the amount of data that can be transmitted. LPWAN technologies exhibit low data transmission rates making them best suited for applications requiring infrequent uplink message delivery of small messages. RFID, which by itself can be considered slow in contrast with WIFI, can achieve speeds up to 640 Kbps opposed to LoRa's 50 Kbps or even SigFox's 100 bps.

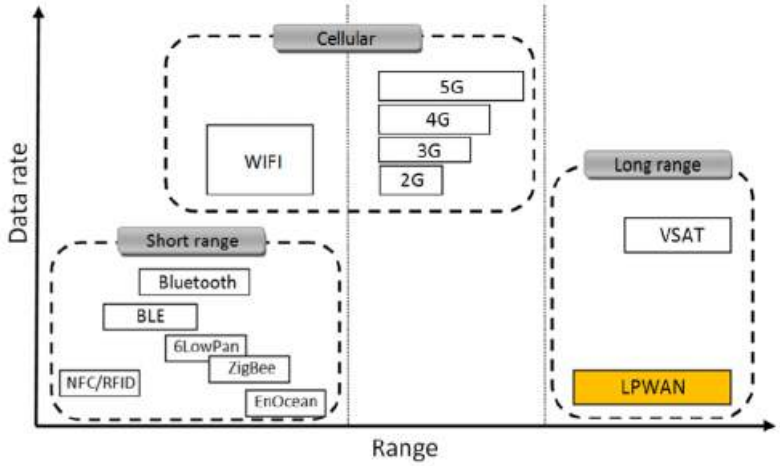


Figure 2.7: Data rate vs range of radio communication technologies [38].

2.5.2 Licensed and Unlicensed LPWANs

Currently the frequency spectrum used for wireless communications, that spans from 3 KHz to 300 GHz, is divided into two categories: licensed and unlicensed bandwidths. Licensed frequencies are reserved for specific use and require consent from the responsible authority (FCC in USA, ANACOM in Portugal, etc) to do so. On the other hand, unlicensed frequencies do not require a licensing fee and are open for free public use. Consequently, networks using the later are cheaper to operate and fast to deploy, but subject themselves to radio wave interference. Due to better signal-to-noise ratios, licensed spectrums carry stronger signals that can travel longer distances but are a scarce resource, difficult and expensive to obtain.

2.5.3 Low Power Wide Area Network Specifications

The LoRa LPWAN solution is composed by two major components, LoRa and LoRaWAN. LoRa is a proprietary physical layer spread spectrum modulation scheme, developed by Semtech, based on the chirp spread spectrum modulation (CSS) technique that sacrifices data rate for sensitivity within a fixed channel bandwidth. This technology operates in the unlicensed ISM bandwidth spectrum below the 1 GHz mark, more specifically in the 868 MHz band in Europe [47]. LoRa achieves data rates between 300 bps and 50 Kbps

depending on the spreading factor and channel bandwidth (2.1) retrieved from [57].

$$R_b = SF * \frac{1}{\frac{2^{SF}}{BW}} \quad bits/sec \tag{2.1}$$

Where:

R_b = Modulation bit rate;

SF = Spreading factor $(7 \cdots 12)$;

BW = Modulation bandwidth (125 kHz, 250 kHz or 500 kHz).

Six orthogonal spreading factor (SF) options are available, from SF7 to SF12, every iteration represents a different compromise between data transmission rates and signal range [38]. Each increment doubles the time on air to transmit the same amount of data, thus the decrease in rate, and increase in the signal perseverance to in band and out band interference noise [39], whilst the decrement of SF will increase the bit rate while sacrificing range. The value of this factor should be decided based on the available bandwidth and signal to noise ratio (SNR). LoRa modulation offers a scalable bandwidth composed by three levels, 125 kHz, 250 kHz and 500 kHz [47], making it capable of performing in both narrowband frequency hopping and wideband direct sequence applications. Additionally, this specification implements a variable error correction scheme that increases robustness by introducing some redundancy [39]. Denoting bit rate as R_b, it can be represented as follows [57],

$$R_b = SF * \frac{\left[\frac{4}{4+CR}\right]}{\left[\frac{2^{SF}}{BW}\right]} \quad bits/sec, \tag{2.2}$$

where

$$Code\ \ Rate = \frac{4}{4+CR} \quad , \quad 1 \leq CR \leq 4. \tag{2.3}$$

CR is the so-called coding rate, BW represents the operation bandwidth and SF is an integer ranging from X to Y.

The period of a symbol (T_s) is defined as [57]

$$T_s = \frac{2^{SF}}{BW}. \tag{2.4}$$

Thus, symbol rate (R_s) is given by the reciprocal of the period (T_s) [57]

$$R_s = \frac{1}{T_s} = \frac{BW}{2^{SF}} \quad symbols/sec. \tag{2.5}$$

Finally, chip rate (R_c) is characterized as [57]

$$R_c = R_s * 2^{SF} = \frac{BW}{2^{SF}} * 2^{SF} = BW \quad chips/sec. \tag{2.6}$$

In essence, the number of chips per second is equal to the bandwidth, 125 kHz of band translate into 125 thousand chips in one second. Increasing the bandwidth will

thereby increase the chip rate and should help the attenuation of the effects caused by heavy multipath fading, which is almost negligible in line-of-sight scenarios [39]. LoRa also inherits CSS modulation resistance to Doppler effect, which causes a small frequency shift of the chip pulse, that in turn introduces a negligible deviation in the time axis of the baseband signal [33]. Messages have a maximum payload length of 243 bytes and a minimum of 59 bytes. Moreover, by employing different spreading factors several messages can transmitted at the same time on the same frequency channel without the risk of communication degradation, notably improving network efficiency and throughput.

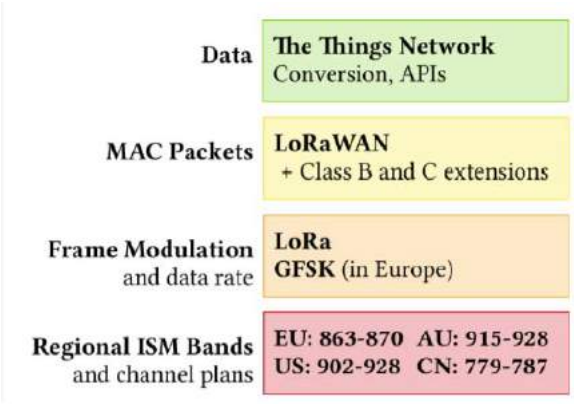


Figure 2.8: LoRaWAN stack [74].

The second component, LoRaWAN, is a network layer medium access control (MAC) protocol, developed specifically for low power end devices (EDs), as indicated in Figure 2.8.

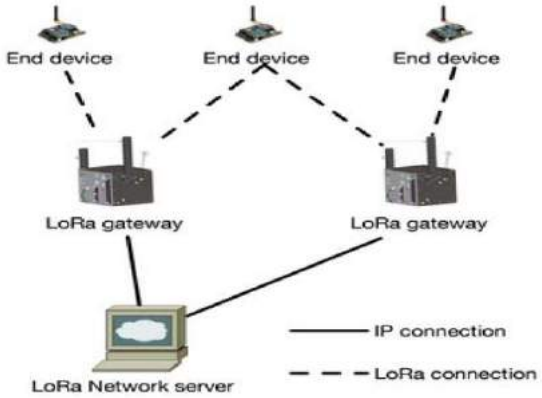


Figure 2.9: LoRaWAN network topology [74].

As noted in Subsection 2.5.1, LoRaWAN, being a LPWAN protocol, operates in a star topology network, in which gateways are used to hand over the messages between end devices and a central core network server (see Figure 2.9). Nodes are not assigned to a single gateway, instead data transmitted by each node reaches several gateways, which in turn forward the received packages to a network server, most likely cloud based as discussed in Subsection 2.1, using a backhaul solution. Messages only travel one hop from

a node to the gateway. Measures against duplicate packages, package security checks and routing to specific applications should be implemented at the gateway or network server.

LoRaWAN defines three distinct end device classes, each with its own MAC protocol (see Figure 2.10), to accommodate trade-off variations between network downlink communication latency versus battery life [66]. Class A offers the best battery life and biggest latency. Class B defines a middle ground, whilst class c devices have the lowest latency at the cost of battery life.

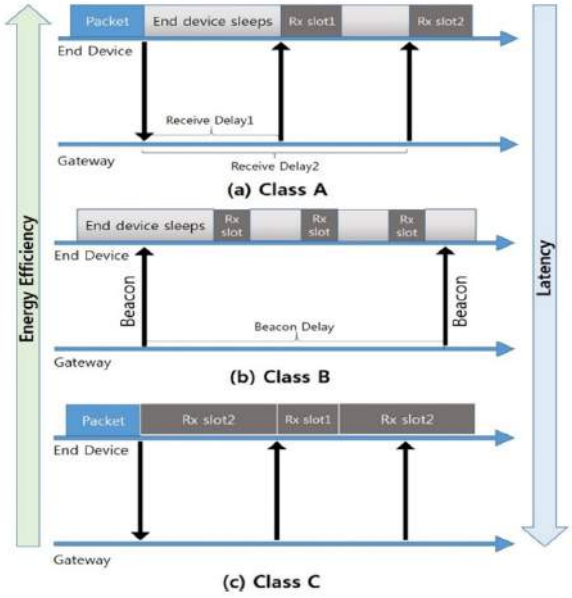


Figure 2.10: LoRaWAN end device classes [66].

- **Class A** - End devices uplink (UL) transmissions are followed by two downlink (DL) receive windows from the server. The first DL frame transmission (Rx1) occurs a short delay after the arrival of the sent package, then followed by the second frame (Rx2). Scheduling is decided by the ED itself based on its needs, similarly to ALOHA protocol. This is the most energy efficient end device class and is ideal for scenarios where DL communication from the server is only needed shortly after a device UL communication. If the server chooses to establish communication with a device at any other given time it has to wait until the next UL transmission. Class A devices are typically, but not exclusively, battery powered sensors.

- **Class B** - End devices are able to receive additional Rx frames during the DL period, at a specified duration, after the arrival of Rx1 and Rx2 frames defined in class A. The duration is established by a beacon frame sent by the gateway on a regular periodic time slot known as beacon delay. Upon receiving a beacon, end devices open a receive window called ping slot, at the specified interval. Essentially, class B devices allow the gateway to control when they should listen. This kind of devices are usually battery powered actuators.

- **Class C** - End devices not only open the two receive windows defined in class A, but also a continuous one until the end of a transmission. Hence, these devices can always receive data, except in the time frame of a UL operation. It has the lowest latency and higher receive capacity for data exchange from the server, being ideal for applications that mainly require downlink operations. Class C devices are the most energy demanding, thus should be used for applications that have a high amount of energy, being able to neglect the need to minimize receive windows. These devices are generally main powered actuators.

In summary, all classes support bidirectional communications. Class A allows downlink communication after every uplink operation, class B enables downlink scheduling and finally class C is always available for downlink transmissions, except when a device has to execute an uplink operation. Class A devices only support unicast messages, whereas the remaining afford both unicast and multicast.

Sigfox is an LPWAN cellular like network that offers an end-to-end IoT connectivity solution for low-throughput applications. It uses Binary Phase Sift Keying (BPSK) as an Ultra Narrow Band (UNB) modulation achieving communication with very low noise levels, low power outlay and efficient bandwidth consumption [46] alongside a bit rate of 100 or 600 bps depending on the region [65]. Conversely to LoRaWAN, Sigfox is not an open protocol by which its use is limited to Sigfox proprietary networks, deployed all over the world.

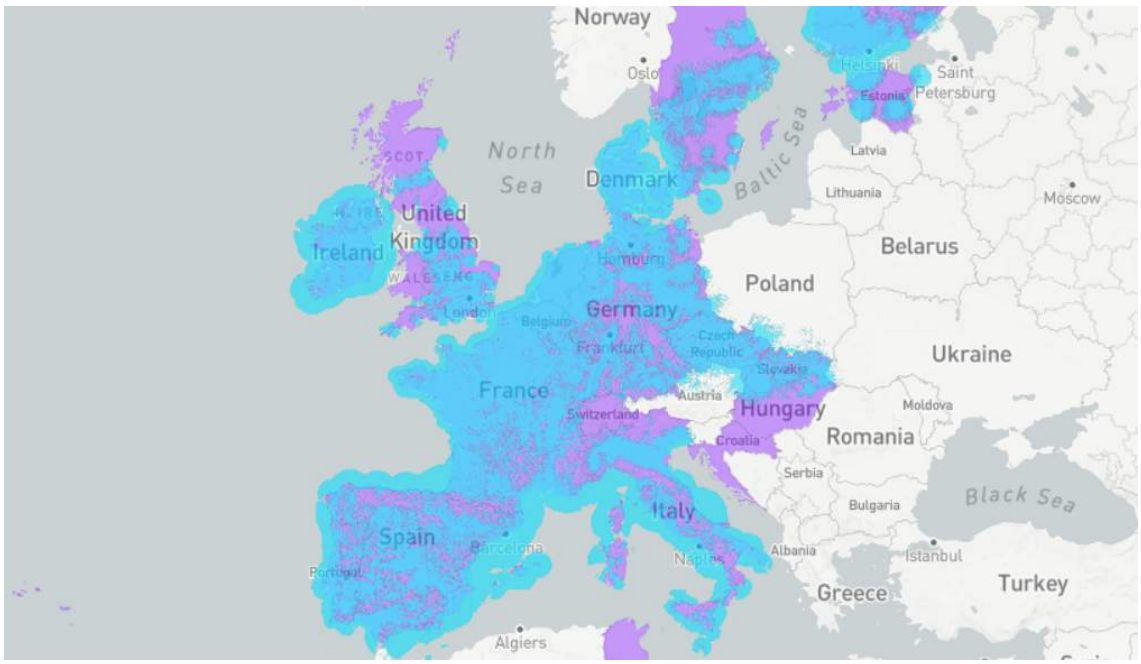


Figure 2.11: Sigfox network coverage in Europe [64].

The UNB fundamental consist in transmitting a signal over a very small bandwidth (less than 1 kHZ), resulting in signals with high power spectral density (PSD) inherently reducing the energy required to trample the noise floor [5]. Furthermore, signals with high PSD have a natural resistance to interference, which proves advantageous in crowded bandwidths. Sigfoxs benefits greatly from these properties since the messages are only 100 Hz wide [65]. In spite of UNB modulation positive effects on the link budget its proprieties are also a source of concern, signals with small bandwidths are particularly susceptible to Doppler effect. Small frequency shifts caused by the variation of the relative distance between a receiver and a source over time can become bigger than the signal bandwidth itself, increasing the probability of message collision as well as hinder its detection/demodulation [5]. To address this issue and increase quality of service, Sigfox implements a random access feature. Each uplink message is sent on a random frequency and then followed by two copies transmitted with a different frequency and time, while base stations search the full unlicensed ISM spectrum (868 to 868.2 MHz in Europe) for UNB signals. This feature also somewhat outlines reliability problems caused by Sigfox lack of message arrival acknowledgment [38]. Downlink messages have to be requested by an ED and can be received upon a twenty second delay after the transmission of the first message, its frequency is equal to the frequency of first frame sent, plus a known delta [65]. Receive windows last a maximum of twenty five seconds. The lack of messages' synchronization between end devices and base stations before a transmission, coupled with ED very low power consumption while idling, are the main factors accountable for Sigfox devices high energy efficiency, thus ensuring long battery life.

Message payload goes from zero (keep alive messages) to twelve bytes in uplink operations, enough to transfer sensor information, GPS coordinates and even some application data. Meanwhile, downlink messages have a static payload size of 8 bytes. European regulations dictate the amount of time Sigfox can occupy the public spectrum to about 30 seconds of transmission time per hour (duty cycle of 1%), resulting in a average of 140 UL and 4 DL messages per day [65].

The overall network architecture is divided into two main layers, the network equipment and Sigfox support system. The former is composed by all the base stations charged with receiving end device messages and delivering them to the later. Sigfox support system layer, as the name implies, enclosures all the support mechanisms necessary to ensure the deployment, operation and overseeing of the network (see Figure 2.12). Its cloud portion provides back-end servers for message and base station monitoring and management, as well as a database for information storage. The web-interface and API section allows customer to access data they collected trough a web browser interface or own information technology (IT) system. Messages are transfered between the two layers through a backhaul that generally uses DSL connectivity and 3G or 4G.

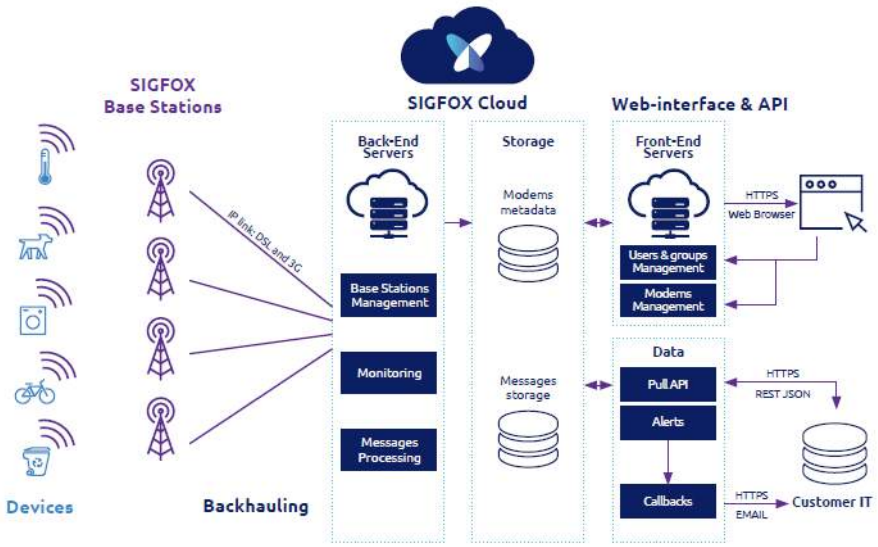


Figure 2.12: Sigfox network structure [65].

NB-IoT is a narrow band cellular Internet of things (CIoT) technology, standardized by the third generation partnership project (3GPP) release 13, designed to offer low device power consumption and cost, improved indoor coverage, low delay sensitivity and the ability to handle a multitude of low-throughput devices [25]. Cellular network protocols are already capable of performing M2M communications, but were not designed to have power constrains nor handle small message transmissions [5], NB-IoT tackles this inaptitude allowing the repurposing of already established cellular networking infrastructures for long range IoT applications. Under these terms, converse to LoRa and Sigfox, this specification operates in the licensed frequency spectrum (700 MHz, 800 MHz and 900 MHz) and was laid out in a way that enables it to coexist with LTE and GSM. As a matter of fact, NB-IoT is essentially a stripped version of LTE protocol, it discards characteristics redundant in an IoT context and enhances the remaining [38]. It occupies a frequency bandwidth of 200 KHz, equivalent to one resource block (RB) in a GSM and LTE transmission [38], and offers three modes of operation (Figure 2.13):

- **Stand-alone** - Refarming of Global System Mobile Communications (GSM) channels. Between each RB of GSM there is an unused 10 KHz interval; remaining on both sides of the spectrum;
- **In-band** - Utilizing resource blocks of a normal LTE carrier;
- **Guard-band** - Take avail of an unused resource block within a LTE carriers guard-band.

Whilst performing downlink operations this specification uses QSPK and OFDMA modulations with sub-carriers of 15 KHz. In uplink, it adopts BPSK or QPSK coupled

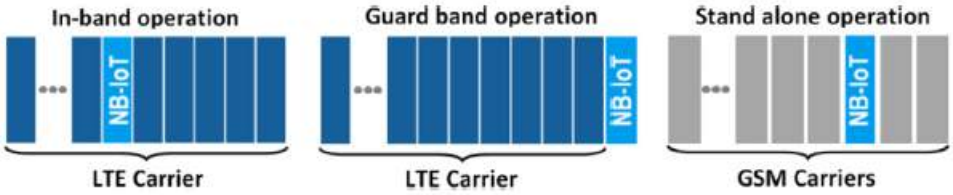


Figure 2.13: NB-IoT modes of operation [38].

with SC-FDMA technology, offering the options of a single or multiple sub-carrier waves, 3.75 KHz or 15 KHz and 15 Khz wide, respectively. Transmissions rates are identical, from 160 and 250 k/bits per second, with the exception of uplink transmissions using single sub-carriers that reach a maximum speed of 200 K/bits per second.

Like LTE, NB-IoT uses the ETSI standard EARFCN to display the carrier channel number and frequency band rather then the actual frequency in Hertz, which can be obtained through equations (2.7) and (2.8). EARFCN values can range from zero to 65535.

$$F_{DL} = F_{DLlow} + 0.1(N_{DL} - N_{off_{DL}}) + 0.0025 * (2M_{DL} + 1) \quad Hz \tag{2.7}$$

$$F_{UL} = F_{ULlow} + 0.1(N_{UL} - N_{off_{UL}}) + 0.0025 * (2M_{UL}) \quad Hz \tag{2.8}$$

where

$F_{DL/UL}$ = Downlink/uplink frequency band;

$F_{DL/ULlow}$ = Carrier lowest frequency in a given band;

$M_{DL/UL}$ = NB-IoT channel number offset for downlink/uplink;

$N_{DL/UL}$ = EARFCN (LTE band and carrier frequency unique identifier) ;

$N_{off_{DL/UL}}$ = Minimum range of $N_{DL/UL}$ for downlink/uplink (lowest defined EARFCN for the band).

NB-IoT follows a common Internet of things architecture, as depicted in Figure 2.14. NB-IoT terminal comprises the sum of all devices integrated into the system. The base stations refers to pre-existing nodes deployed by telecom operators. Usually these support all three of the aforementioned modes of operation. Core network behaves akin to a bridge, enabling connections between BS and a cloud platform. The cloud platform offers and performs a plectra of services then forwards outputs to the vertical business center whose function is up to the client. Typically this layer contains GUI for viewing of data collected by the system as well as control mechanisms for actuators or any other device embedded into the terminal layer.

	LoRaWAN	**SigFox**	**NB-IoT**
Modulation	CSS	BPSK	QPSK
Spectrum	Unlicensed ISM bands	Unlicensed ISM bands	Licensed LTE frequency bands
Frequency Europe	868 MHz	868 MHz	Licensed LTE frequency bands
Frequency North America	915 MHz	915 MHz	Licensed LTE frequency bands
Frequency Asia	433 MHz	433 MHz	Licensed LTE frequency bands
Bandwidth	125 kHz 250 kHz 500 kHz	100 Hz	200 kHz
Maximum message payload	59-230 bytes	12 bytes (UL) 8 bytes (DL)	1600 bytes
Adaptive data rate	Yes (SF dependent)	No	No
Range	5 km (urban) 20 km (rural)	10 km (urban) 40 km (rural)	1 km (urban) 10 km (rural)
Authentication and encryption	AES 128b	Not supported	LTE encryption
Private network option	Yes	No	No
Standardization	LoRa-Alliance	Currently in the works with ETSI	3GPP

Table 2.4: Overview of LPWAN technologies.

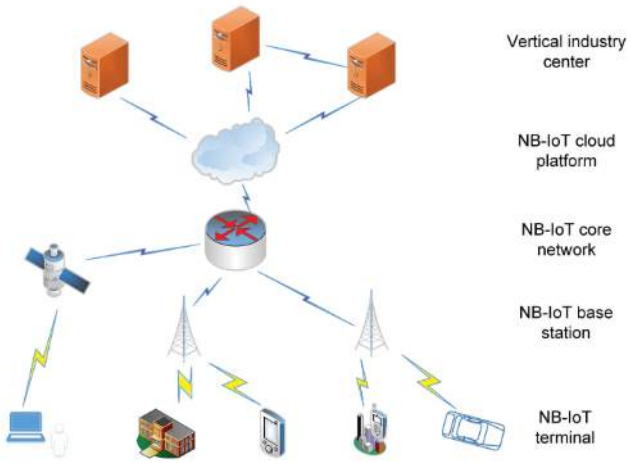


Figure 2.14: NB-IoT network structure [12].

2.6 Cloud Computing

Currently there are several storage service solutions available in the market, where three different models of ready to use cloud services are recognized: *Infraestruture as a Service* (IaaS), *Software as a Service* (SaaS) and finally *Platform as a Service* (PaaS) [11, pp. 10-11].

These can be made available in three distinct ways [11, pp. 10-11]:

1. **Public Clouds** – Cloud services are handled by a service provider accessible to the general public. This kind of Cloud is owned by third party companies, who are in charge of administering and maintaining its infrastructures, providing only access to its services via Internet;

2. **Private Clouds** – Are built merely for the exclusive use of a client/organization. This means an increase in cost, but offers an unprecedented control over security settings. They may or may not be administered by a third party company;

3. **Hybrid Clouds** – A combination of the models described above.

Scalability, usability, reliability, security and finally costs, are all factors that weight in the decision of which model to use.

Figure 2.15, illustrates the hierarchy of the cloud computing paradigm. The authors also specify the top layer, *Software as a Service*, as being the one responsible for integrating information from systems and devices, since it is the layer that offers services to the final user. The blocks integrating the *Platform as a Service* contains operating systems, databases and application serves. Finally, the *Infrastructure as a Service* is composed by data centers, clusters and networking.

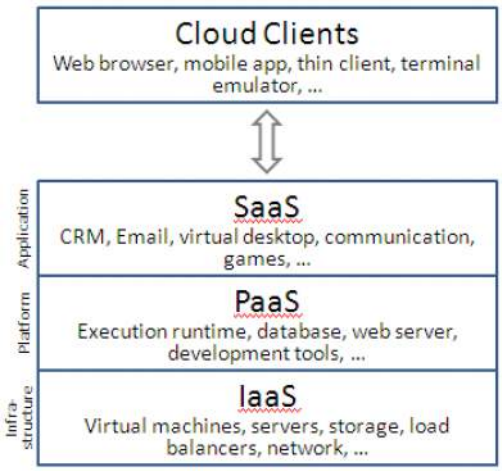


Figure 2.15: Overview of the central elements of cloud computing (adapted from [70]).

2.7 Databases

A database stands as an assortment of organized information allocated either locally or in a virtualized environment like a cloud, fundamentally conceived not only with the purpose of data storing, but also as platform to facilitate data access, update and management. These can be of two types, Relational or SQL and Non-Relational or NoSQL databases.

2.7.1 Relational Databases

Relational databases use Structured Querying Language (SQL) and are organized according to the relational model of data, proposed by Edgar Frank Codd in the seventies. Information is organized into tables of rows with an unique key, representing an instance of an entity, and columns of values of said identity. Keys, which are used to uniquely identify any atomic piece of data within that table, can be primary keys if they belong to the table itself, or foreign keys when borrowed from other tables. Thereafter, storing a foreign key allows information from different tables to be linked.

One of the most substantial features of relational databases its the implementation of ACID (Atomicity, Consistency, Isolation and Durability) properties which reinforces transaction reliability and preserves data integrity [45]:

- **Atomicity** - Every transaction is unique and in case it fails, all changes are nullified, returning data to its previous form;
- **Consistency** - All information contained within the database is governed by the rules in place (constrains,triggers, etc..);
- **Isolation** - Transformations performed by transactions are not visible until completed;

- **Durability** - All modifications applied by transactions are stored and available even if the database suffers a deficiency (power failure, connection drop, etc.) .

2.7.2 Non-Relational Databases

Non-Relational databases dispose of the referential integrity of the previous model with the intention of decreasing complexity and increasing horizontal scalability, in order to handle rapidly growing unstructured data. This scheme follows the CAP (Consistency, Availability and Partitioning) proprieties, but is only capable of guaranteeing two at a time:

- **Consistency** - All the servers in the system have the same data, regardless of which server respond to the request, the answer will be identical;
- **Availability** - Requests must always be answered, even if the data is outdated;
- **Partitioning** - In the the event of an individual server failure the system must continue to operate normally.

Additionally, since Non-Relational databases do not follow the traditional architecture, they can be classified into four data model categories:

- **Key-values database** - Every single item stored in the database is associated with a key;
- **Column database** - Data is stored in columns, that in turn are spread over a cluster;
- **Document database** - Pairs keys with complex data structures, called documents;
- **Graph database** - Uses nodes and edges to represent stored data in graphical form.

2.7.3 Overview

Relational databases like MySQL and PostgreSQL have the advantage of being able to handle intricate querying, and database transactions more efficiently than its counterpart. Specifically, applications that heavily rely on transactions can maximize their reliability and ease of management by employing a relational model. Likewise, index capabilities grant users a sophisticated way to access and manipulate stored data enabling both operational and analytic applications. However, when dealing with extensive amounts of data or simply complex unstructured data, Non-Relational models, like MongoDB, have the upper hand. These store information without explicit structures, avoiding the need for de-normalization of database schemes, increasing performance and scalability.

2.8 Data analytics

Since the past decade, the ever increasing volume of IoT systems coupled with the rise of social media and smartphone adoption [21] have produced extensive amounts of data inducing the blossom of new business practices that spread over all areas of technology, essentially turning big data analytics into one of the biggest and fastest growing global markets [36]. As the name implies this paradigm does not engage in database populating or data collection, it is strictly aimed at information mining. Data analytics is the amalgamation of processes to which said information is subjected in order to produce insight, such as hidden correlations among a system, behavioral patterns, trends, etc... Thus it includes analytic algorithms and data visualization mechanisms (graphs, charts, tables, etc) that display the findings. Additionally, this technique not only enables a better understanding of a system intricacies, but also helps making predictions or even unfolding unknown information, facilitating efficient decision making and the development of new technologies. Healthcare and medical industries, smart cities, energy smart meters, miscellaneous monitoring systems are only a few examples of areas that can benefit greatly from such algorithms [36].

2.8.1 Types of Analytics

Data can be handled several different ways, depending on the system requirements, as well as its processing capabilities. Arguably it would be ideal if every system was powerful enough to process all the collected data in real time, but such is not possible due to both hardware and software limitations. Nonetheless, when very low latency of response is required, real-time analysis is the answer [44]. This kind of analytics is typically performed on data collected by sensors, considering these produce a reasonable amount of information at manageable rates allowing analytic algorithms to keep up and avoiding data amassing that ultimately will clog the system and spoil the response time. Continuous real-time analytics is more demanding but in return enables proactive responses, allowing a system to engage triggers, alert users and so on, based on current events[22]. On the other hand, an on-demand approach applies less constrain on a system but its utility is more limiting, it has to wait for a query request and only then analyses the current data and delivers the results [22]. Currently, there are two real-time architectures: memory-based computing platforms like SAP Hana, where data is processed where it resides, refereed to as in-memory processing; and parallel processing clusters planted on a relational database offered by solutions like Greenplum [36] and Cloudera. Memory level analysis is conceptually dependent on the available memory, problem that can be somewhat bypassed with the aid of data stores like MongoDB.

Alternatively, some applications do not require quick response times, and have much to gain from employing off-line analysis. This method is widely adopted by Internet enterprises as an effort to reduce data format conversion expenses. Many implementations are Hadoop

based, essentially instead of performing data analysis on one physical storage device, this can be achieved much faster and efficiently using many smaller devices connected to a cloud. Examples of architectures that follow this paradigm are platforms like SCRIBE and Kafka [36].

When data size reaches proportions on the Tera-byte level, theres Business Intelligence (BI) analytics approach, more directed towards business feedback extraction, market predictions, etc... BI analytics encompasses a wide variety of tools, that handle data collection, perform analytics and provide dashboards as well as other data visualization mechanisms. Usually, the studied data is not exclusively extracted from within the system, but also from external sources allowing for more detailed results, assuming outside data has been properly adapted and integrated into the system. When employed correctly, BI analysis can potentially accelerate and improve decision making, find system faults, increase operational efficiency and so on, as a result is one of the more widely adopted data analysis types.

In some extreme cases the scale of data exceeds even the capacity of BI analyses and traditional databases. Projects like the Large Hadron Collider (LHC), the particle accelerator that is capable of producing around sixty Tera-bytes of data per day, or the decoding of human genome, whose information load was so large that it took a decade to complete [44] require intense processing power accompanied by copious amounts of storage space. In this kind of scenarios it is necessary to use massive analytics, a method that uses Hadoop distributed file system (HDFS) for data storage and Map/Reduce computational paradigm for analysis [36]. Map/Reduce, pioneered by Google, functions by splitting a complex problem into several sub-problems, until each of them is scalable for solving directly. After solving every sub-problem, separately or in parallel, the solutions are then combined resulting in the solution of the original problem [44]. This type of analysis is essentially a bigger scale and more complex version of BI analysis.

2.8.2 Analytic methods

Data analytics is employed in both statistical and machine learning applications, accordingly several suitable solutions and methods (see Figure 2.16) exist to cover each particular scenario necessities.

Classification and class probability estimation is a supervised learning approach that aims to predict, for each individual set of data, to which set of categories it belongs. Being a supervised method means the systems do not create their own categories but rather classify data based on previously defined groups. In small data samples, patterns are easily identifiable, sometimes even evident to the naked eye, however the sheer amount of information involved in big data imposes the use of more complex methods like Bayesian networks, support vector machines and k-nearest neighbor [36]. Bayesian networks are a relative of probabilistic graphical model capable of building models from feed data [61], these are most adept at breaking down complex data structures generated through big

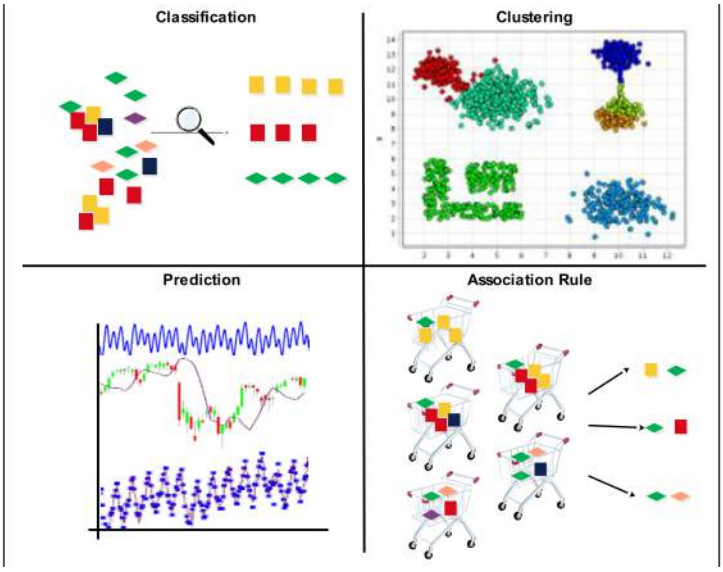


Figure 2.16: Data analytic methods [36].

data. Support vector machines (SVM) through the use of statistical learning techniques are able to analyze data patterns and effectively sort similar information into conglomerates, essentially defining categories. The k-nearest neighbor (KNN) algorithm is an alternative to SVM, considering its effectiveness in pattern discovery when dealing with big data samples. As a whole classification techniques are extremely predominant in big data analytics, applied in several scenarios, like text classification, pattern matching, commerce, anomaly detection, etc.

Clustering is another prevailing big data analytics method, but contrary to classification, uses an unsupervised learning approach. Rather than assigning individual samples to a preexisting group, it searches for distinctive and meaningful characteristics among a data set, then creates groups into which data is distributed [36]. There are two clustering approaches: partitional and hierarchical clustering. The distinction is whether the cluster is nested or unnested. In hierarchical clustering, clusters are nested and organized in a tree formation, whereby a single data object can correlate to several clusters [48]. Trees can be built from the bottom up (agglomerative clustering), where each point starts as an individual cluster and the closest pair is merged together with every iteration, or from top down (divisive clustering) where an all-inclusive cluster is divided every iteration until only clusters of individual points remain. This method proves to be very efficient at identifying hidden taxonomies that may exist within a system, by contrast, cluster merges are final, crippling all future optimization attempts. Additionally, hierarchical clustering requires an affluence of computational power and storage space, increasing operating expenses. All-rules algorithm and AGNES are two of the more prevalent algorithms used in this approach. In partitional clustering data is organized and divided into non-overlapping clusters, as so, each data object belongs to one and only one subset. This method enables the production of straightforward and precise rules that describe data objects within a

data set, in view of this, the fact that these rules may only be able to represent a very small subset of data can be derogative when dealing with extensive amounts of information [48]. Some of the algorithms used to accomplish this are k-medoids, PAM and CLARANS.

Predictive analysis, as the name implies, aims to predict behavioral trends using previously obtained data, also known as training data. Combined or independently, SVM and fussy logic algorithms interpret relationships between dependent and independent variables, enabling the formulation of regression curves. This method is useful in a plectra of situations, being employed is natural disaster prediction facilities as well as more mundane scenarios like customer buying predictions, online trends and market demands.

Association rule method aims to find associations between items of a set of transactions. In turn each transaction contains a set of items, called itemset [75]. Rules are implications defined as $x \rightarrow y$, where x is called left hand side (LHS) or body and y is the right hand side (RHS) or head [29]. Both x and y are itemsets that do not share common items. Essentially, the body represents an antecedent while the head is its most probable precedent. This method defines the probability of a precedent in two distinct ways: support represents the probability of x and y, while confidence dictates the probability of a transaction containing x and y. Supposing one of the rules dictates that when people buy bread there is an high chance they will also buy butter, if in a sample of one hundred transactions, twenty of them are of bread and in nine of those transactions people also bought butter, then:

$$Support = \frac{20}{100} * 100 = 20\% \tag{2.9}$$

$$Confidence = \frac{9}{20} * 100 = 45\% \tag{2.10}$$

Several algorithms like, Apriori, Charm, MagnumOpus were all explicitly designed to accommodate the previously described specifications, thus rule generation is handled in the same way. Firstly, generation of all frequent itemsets, then rule construction based on existing itemsets.

As a whole, these methods are able to cover most of the marked necessities, thus their relevance and wide adoption rates in the big data spectrum. Seamlessly the conclusion that can be drawn from this brief description echoes the outcome of Subsection 2.4.2. On no account is possible to pinpoint an ubiquitous solution, instead the focus should be on the system computational capabilities, scalability requirements, and naturally on the desired end result.

2.9 IoT architectures

When designing an IoT system there is an overwhelming amount of technologies and options to choose from. Nonetheless there are several prerequisites, embedded into this concept, that have to be met [52]:

- **Automation** - Automation stands as the most crucial feature of any IoT infrastructure. These systems must support object collaboration, autonomous data collection and decision making mechanisms;
- **Intelligence** - Intelligence should be built into every network object, empowering them to adapt to different operating conditions, minimizing the need for human action;
- **Dynamicity** - IoT systems should be able to dynamically detect when an object change its position or environment and adapt to the situation, essentially ease of object integration must be equal all over the reach of an IoT ecosystem;
- **Lack of configurations** - Not always possible, but IoT should support plug and play features whenever possible, in order to promote decentralized growth.

The core purpose of IoT is to provide ubiquitous computing, but the level of heterogeneity linked to the infinitude of available devices coupled with the lack of standardization makes interoperability an highly complex goal to achieve. By the same token, as specified in Subsection 2.3, standardization is held back not merely by the diversity of devices, but in equal ways by all the divergent requirements of each IoT system and may never be a reality. Fortunately, the rise of middleware solutions has somewhat mitigated this issue. This concept acts akin to a software bridge between objects and applications, in essence, it provides hardware abstraction accompanied with an application programing interface (API) that enables and handles communication, data management, computation and security with scalability in mind [62]. Middleware platforms divide interoperability into three types, network, semantic and syntactic. Network interoperability offers heterogeneous interface protocols for device communication. Syntactic interoperability makes an application unaware of data formats, structure and encoding. Semantic interoperability abstracts the meaning of data within its domain [62]. Device discovery mechanisms and object awareness are enforced by requiring objects to announce their presence and provided services. Complementarity, many of these solutions have big data analytics and cloud services embedded, effectively reducing the afford required to employ such features.

Nonetheless, even if solutions like middleware frees developers to concentrate their focus on application requirements rather then on hardware integration, some systems benefit from or require proprietary solutions, thus this matter remains highly complex and theres still challenges to tackle [52]:

- **Heterogeneity** - Devices have different functions, operating conditions, specifications, among others, making it increasingly harder to seamlessly integrate devices as their numbers grow;
- **Scalability** - The expeditious growth of devices which correlates in an massive increase in collected data volume is becoming progressively more demanding to handle and requires sophisticated data storage solutions;

- **Interoperability** - As stated above, the lack of standardization coupled with a wide diversity of devices continues to cripple object interaction within IoT systems;

- **Security and Privacy** - The heterogeneity inherent to the IoT concept hinders the implementation of security measures like, data authentication, data usage control and data protection. Furthermore, the rise of data analytics has brought privacy concerns regarding to what extent data collection can be harmful to users or even if personal data should become personal propriety, subject matter that still has not reached a consensus.

2.9.1 Service Oriented Architecture (SOA)

The SOA paradigm is directed towards the interoperability between the heterogeneous elements in a system [51], it abstracts services from their providers and implementations. A service is a discoverable resource, with an externalized description available to clients (service consumers), that are offered by service providers (sensors, software, etc.) [6]. Clients or service consumers can perform actions without the need to know what processes are involved. They can simply search and invoke services by their description. Services are independent and deal with their own operational logic and associated data, but can be interconnected with each other to accomplish more complex tasks [7].

Three levels of abstraction can be defined within this architecture [77]: operations, services and business processes. Operations constitute the straightforwards tasks, usually read, write or modify procedures. Services are logical conglomerates of operations, for example a service that would display an order details would evoke several read operations like customer name, address, phone number, and so on. Finally, business processes encompasses lists of services to accomplish a determined business goal. This detachment grants the system the ability to add, replace or modify physical devices or software, responsible for the aforementioned services, without disruption its operation, thus fulfilling the scalability and flexibility requirements of IoT.

Service oriented architectures, like every IoT composition, are not defined by or confined to one universal design, but all systems that follow this paradigm share service loose coupling (services or service providers can be implemented, replaced or modified without causing prejudice to the system), service abstraction (consumers are unaware of the intricacies involved within a service) and service autonomy [51].

A basic SOA design is depicted in Figure 2.17. It features a sensing layer responsible for hardware integration and abstraction, a network layer that handles all communication while enforcing quality of service, energy and security measures, which can be implemented by a gateway. A service layer responsible for service management and advertising. Finally, an interface layer with a built-in GUI is used to display the available services, functions and achieved outputs, tasked with communicating to the bottom layers.

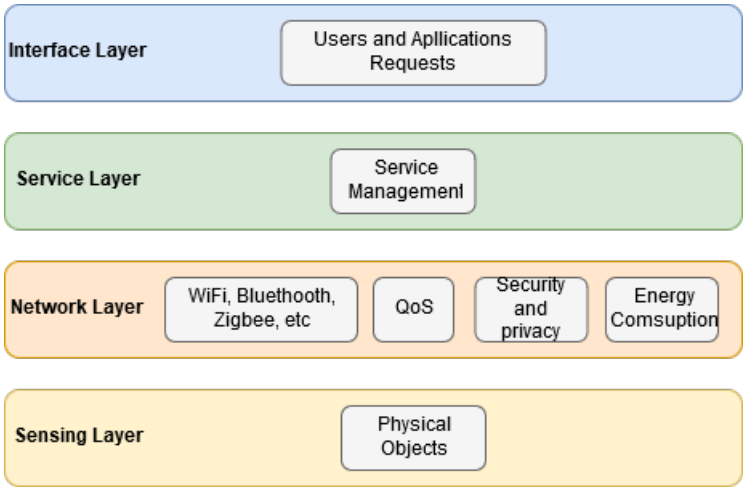


Figure 2.17: Four-layer service oriented architecture.

2.9.2 Distributed Internet-like Architecture for Things (DIAT)

DIAT, depicted in Figure 2.18, is an architecture inspired by the SOA principles, proposed by the authors of [52]. It is composed by three main layers (VOL, CVOL and SL) and a cross layer security module:

- **Virtual Object Layer (VOL)** - As suggested by the name, this layer virtualizes physical devices, akin to a sensing layer in a SOA system. It holds unique virtual representations of every object, known as Virtual Objects (VO). Each VO has a semantic description of its own capabilities and features, enabling the use of global procedures to access all connected physical devices, effectively dealing with heterogeneity concerns. Essentially, a VO can be interpreted as a translator between the physical and the cyber worlds, the path to access a device, while the VOL is the bridge that connects both worlds;

- **Composite Virtual Object Layer (CVOL)** - Some tasks can not be accomplish by a single VO, but are easily solvable through a conjoined effort. This layer is task with managing and coordinating such efforts. When it receives a request, the CVOL creates a Composite Virtual Object (CVO), which consist in a mash-up of VOs whose capabilities were deemed by the layer as necessary to complete its task. The CVO will then act as an coordinator, by dictating how and when each individual VO should work. Furthermore, in order to identify which group of VOs possesses the means to achieve the desired results, this layer is equipped with a discovery mechanism that constantly scans the aforementioned device semantic descriptions;

- **Service Layer (SL)** - The SL is in charge of service creation and management. It takes users service requests, analyses and splits them into a description list of smaller subtasks, that is then forwarded to the CVOL layer to be executed. This layer also features automatic service creation based on context;

- **Security Management (SM)** - The SM module is a cross layer security enforcer. Its primary aim is to control data usage, resources consumption and services of the integrated objects.

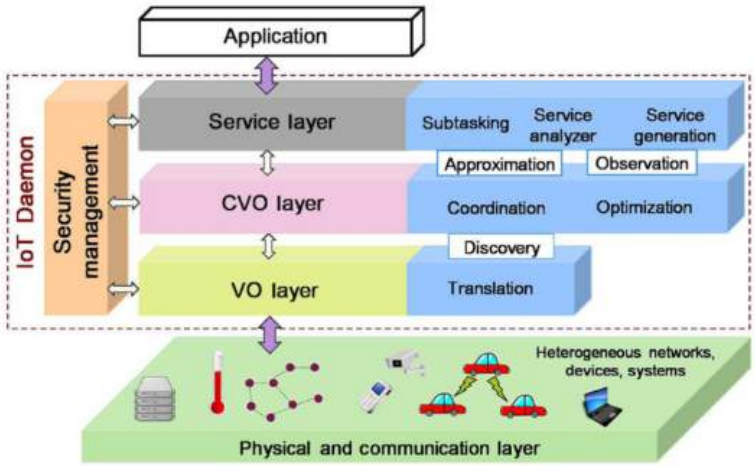


Figure 2.18: DIAT architecture [52].

To achieve automatic service creation on the service layer, the authors define a cognitive entity, refereed to as the observer, whose reach is spread across both the SL and CVOL. This entity continuously collects the contextual data of each object and stores it respectively in an unique associated vector. Objects are split into two categories, human and non-human, thus their data is store into two different types of vector (Figures 2.19 and 2.20) in accordance with their assigned category. This information allows the system to react accordingly to its present state and dynamically create suitable services, for instance when dealing with a human object, the stored contextual data (Figure 2.19) is the following:

- **Current location** - This field contains the relative physical location of a human being, instead of exact gps coordinates, it stores positions known within the system, like atBedroom, atOffice and so on. Its sub field, expected location, holds similar information but its value is dictated by previously scheduled jobs or even by observer inputs;

- **Operating state** - Indicates the current activity a person is engaged in (inMeeting, isWorking, etc.). Once again its sub field contains the next pre-scheduled activity;

- **Next job queue** - Holds upcoming jobs, extracted from the to do list associated with a person. It has two subfields, notification time which indicates the approximate time when a event should start (SL launches a new service request) and complementary service which indicates jobs in queue. Jobs placed in this queue are complementary services, necessary to complete the next upcoming task;

- **Interruption** - It is a flag used to stop the execution of a service if human intervention is required. Depending on the urgency of a situation and on the operation state of a person, notifications can be immediate or postponed till an appropriate time arrives.

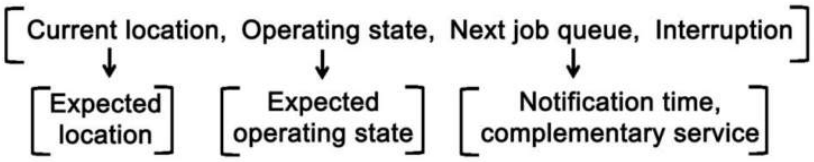


Figure 2.19: Human object contextual vector [52].

By comparing these fields, for example, in the eventuality of a mismatch the system, using the current location field, can perceive that a person wont be able to reach the expected location and create a service to reschedule an appointment or inform specific people that the subject will miss a meeting, etc... Operation state field can avoid disturbances like phone calls while a person is unavailable at work. Interruption flags can be crucial in emergency situations. In home environments, notifications from events like light malfunctions can be postponed, while burglary or fire situations should be immediately transmitted to the owner, regardless of their current status. Succinctly, dynamic service creation is driven by explicit conflicts in the information collected by the observer. The same logic applies with non-human objects, where the contextual vector fields (Figure 2.20) are as follows:

- **Attention flags** - A collection of flags that specify if an object needs attention, in the eventuality of an anomaly. Attention is not exclusive to human intervention, it may refer to a need of communication with other objects. Additionally, the value of a flag also signifies the urgency of a situation and how quickly it should be dealt with. As a case in point, if the observer interprets the data from a fire detector VO as indicative of a fire, it sets the attention flag to a value such that an immediate fire alarm service request is started;

- **Working neighbor group** - A group of objects with similar capabilities within the same relative geographical location. Affiliates can communicate amongst themselves for coordination and performance improvements;

- **Collocation neighbor group** - Similarly to the above description, a group of object that share the same relative geographical position, the difference being that capabilities are not taken into account.

As previously described, the execution of requested services is the responsibility of the composite virtual object layer. The dynamics introduced in the system by the observer can hinder the execution of services in real time. To counteract this issue, a policy

Figure 2.20: Non-human object contextual vector [52].

based model was proposed. Policies, also created dynamically based on observer inputs, denote a structured way of establishing which CVOs are required to complete a service request. Generically speaking, the data structure of a policy is composed by: policy id, modality, trigger, subject, target, behavior, constraint, role, desires, intentions and assignment. Policy id, self evidently, is an unique identifier of each policy. Modality defines the authorizations and obligations of VOs. Trigger defines time events or VOs states. Subject and target define the purpose of the VOs within the system. Behavior defines the long-term goal of a policy. Constraint specifies the circumstances where the policy is enforceable. Role defines the functions needed to achieve the goal. Desires stores the group of subgoals derived from a service decomposition. Intention dictates how subgoals should be executed, this field can be dynamically updated based on the availability of VOs. Lastly, Assignment is dynamic mapping mechanism that assigns roles to VOs whose capabilities are a necessary step to achieve a goal.

These are split into three categories, one for every layer of this architecture:

- **High-level policy (SL level)** - Handles macro-level specifications of service requests.
- **Concrete policy (CVO level)** - Determines the subgoals of a service and the functions of VO. Essentially, it defines how a CVO should be created to achieve a specific goal;
- **Low-level policy (VO level)** - Determines function of the each VO in the system, by storing their implementation details.

Furthermore, to define policies for dynamic service creation the authors developed a belief-desire-intention-policy (BDIP) model, depicted in Figure 2.21. It features 4 main entities:

- **Belief** - The initial belief on how the CVO should behave to accomplish the goal;
- **Desire** - The goal that the CVO needs to achieve;
- **Intention** - The sequence of actions needed to achieve the goal;
- **Policy** - How to execute the sequence actions and the roles of each individual CVO and VO.

Based on service history logs and the current service request, the BPIP model is able to determine its initial belief. Using this, it updates the desire entity with the current

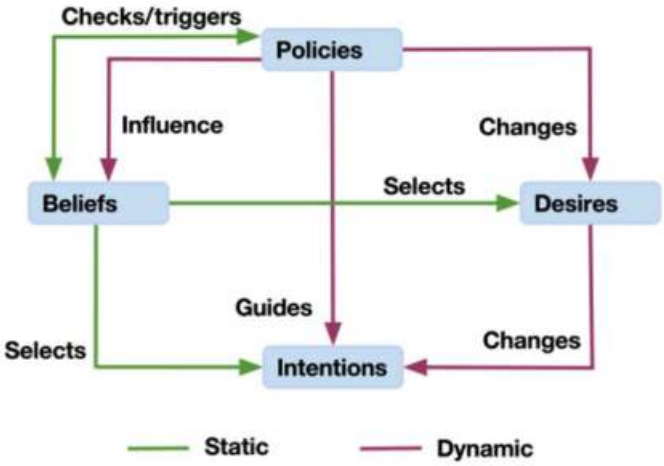


Figure 2.21: DIAT architecture BDIP mode [52].

goal and a plan of action (Intention) is delineated. Concurrently, the observer monitors virtual objects and generates new service request whenever it deems it necessary in order to accommodate dynamic environment changes. These new service requests cause policies to influence the initial belief, thereby indirectly triggering a new CVO goal (Desire) that in turn will affect Intention.

Finally, the cross layer module known as the security management module is composed by three components (see Figure 2.22). A policy repository (PR) stores the multiple policies. A policy manager (PM) tasked with collecting policies from the PR and sending them to the policy decision point (PDP). The PDP subscribes to events in the policy enforcement point (PEP) and enforces policies. The PEP is a layer and technology specific module whose job is to acknowledge and report events to the PDP. Events are detailed descriptions of actions being executed as well as interactions among objects (VOs and CVOs) and all the other involved entities. The PDP, subsequently to the notification of an event, tells the corresponding PEP how it should act using a policy language consisting of four commands (allow, deny, modify or delay).

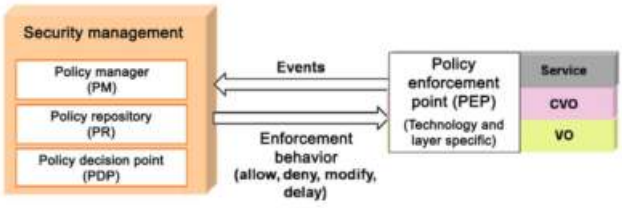


Figure 2.22: DIAT security management module [52].

2.9.3 Semantic Service Oriented Architecture (SSOA)

A semantic IoT architecture was suggested in [72], to tackle interoperability issues, mentioned in Subsection 2.3.1, at an application level. The paper proposes the implementation

of a gateway at the network level, essentially, between the hardware or physical level and service level. The gateway is described as a semantic gateway as service (SGS), a bridge between devices and IoT services, capable of translating application level protocols (MQTT, CoAP, etc), thus enabling interoperability.

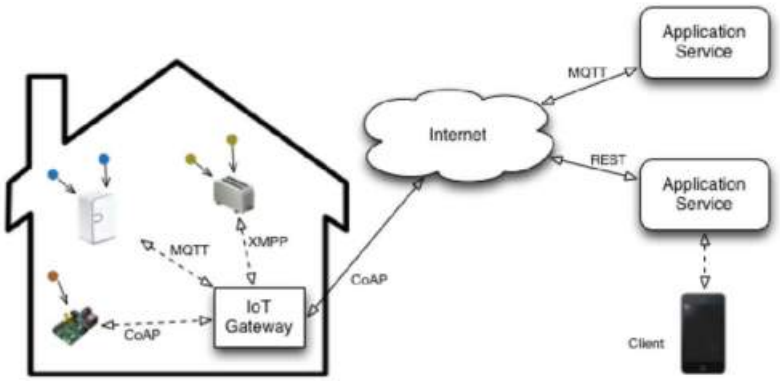


Figure 2.23: Semantic IoT architecture [72].

This architecture features a common wireless sensor network topology, sensors and actuators connected to nodes, which in turn are connected to sink nodes also known as end-points. These sink nodes then connect to the gateway, using one of the aforementioned protocols. The data is transfered upwards in its raw format (without any semantic annotation). As of data arrival, the gateway stores the corresponding sensor semantic information, essentially exposing their services to front-end applications. As observable in Figure 2.23, communication between the gateway and applications uses REST or publisher/subscriber based protocols.

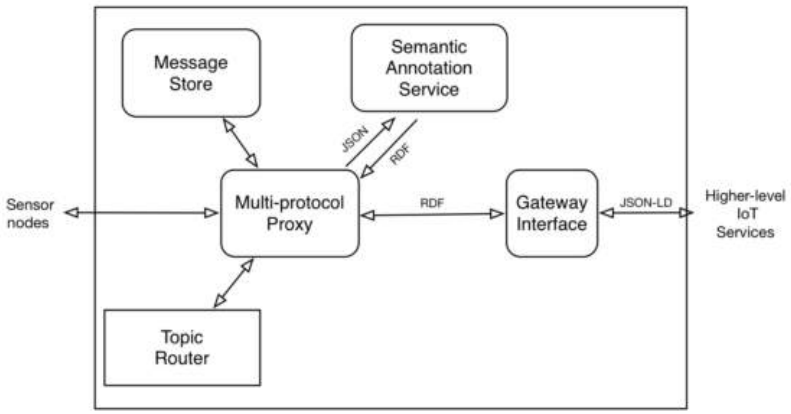


Figure 2.24: Semantic gateway as service [72].

The main component in the SGS module is the multi-protocol proxy, responsible for message translation, jointly with the message store and topic router components. Whenever

a sensor generates data, it is sent to the gateway, and enters the proxy. The proxy contains protocol specific interfaces where messages are normalized. In other words, if the end points communicate using either CoAP and MQTT the proxy will provide a CoAP server and a MQTT broker where corresponding messages will be translated to an universal format and placed in a general message broker. Afterwards the message is stored in the message store, whose role is to save the last message of every publisher to guarantee QoS, and a list of corresponding subscribers is fetched from the topic router. Upon receiving the list of subscribers the message is once again translated to the format supported by each subscriber and forwarded, if it is meant for another sensor node, otherwise it is sent to the gateway interface module. In the eventuality where node subscribers share the protocol used by the publisher, messages bypass the translation stage and are directly forwarded.

Semantic annotation is handled by the semantic annotation service (SAS) module. Messages that reach the message broker, prior to being forwarded, are processed by this component. Annotation provides standardization at three levels: service description and discovery, sensor and observation description, domain specific descriptions; The first utilizes the Open Geospatial Consortium Sensor Web Enablement (SWE) standard specifications, O&M and Sensor Model Language (SensorML) provide a standard model and XML schema for sensors processes and measurements, while the sensor observation service (SOS) offer querying mechanism for observations and sensor metadata. This allows services to be dynamically discovered by other services within the system. Sensor and observation description is provided by the semantic sensor network (SSN) ontology, developed by W3C. Each message is annotaded with sensor description, allowing software and applications to handle these while maintaining semantic abstraction. Lastly, domain specific descriptions refer to this architecture support of domain specific technologies if it intended purpose requires so.

CHAPTER 3

LoRa and LoRaWAN

3.1 LoRa

3.1.1 Encoding

3.1.1.1 Whitening

Ubiquitously, data impending transmission is grouped into packets, as a result, these may contain lengthy sequences of 1's or 0's, introducing a DC bias in the sent signal. The bias causes a non-uniform power distribution over the used channel bandwidth. The solution to this problem is the randomization of data [73].

Two main approaches are Manchester encoding and data whitening. The former ensures the absence of more than two consecutive 1's and 0's. However, this process greatly hinders the system performance. It doubles the amount of transmitted data, effectively halving the bit rate. The latter, used in LoRa, consist in XORing data with a random whitening sequence. On the receiver side, data is de-whitened using this same whitening sequence. The specification limits the number of consecutive 1's and 0's to nine and is only employed if the data is not already randomized [73]. Moreover, whitening sequence can be reveled by transmitting a frame of zeros.

When whitening is used, the addition of a 2 byte Cyclic Redundancy Check (CRC) checksum to the payload is mandatory, thus enabling the validation of the received data [73].

3.1.1.2 CRC

CRC, also called polynomial code, handles bit strings as polynomials whose coefficients can strictly be one or zero. A k bit string is treated as list of coefficients for $k-1$ degree polynomial with k terms. The most significant bit is the coefficient of x^{k-1}, the next bit

is the coefficient of x^{k-2} and so on, till the least significant bit, i.e. coefficient of x^0 [71]. For instance, the string 101101 represents:

$$1x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0$$

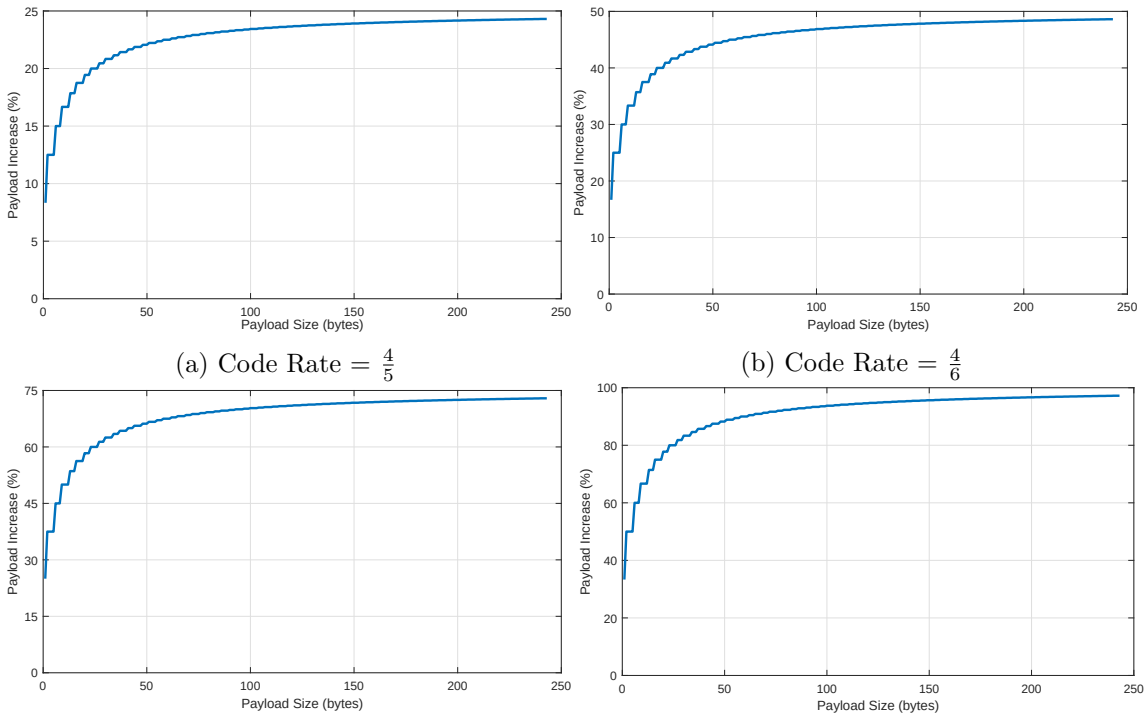
When polynomial code is in use, receivers and transmitters must agree on a communal generator polynomial $G(x)$, whose degree must be smaller than $M(x)$, whereas $M(x)$ is the polynomial correspondent to the frame of m bits to be transmitted. Considering g the degree of $G(x)$, g zero bits are appended to the least significant bit end of the string of bits to be transmitted. Now it contains $m + g$ bits and its polynomial is $x^g M(x)$. This string is divided by the bit string corresponding to $G(x)$ using modulo 2 division, which is identical to binary long division, except addition and subtractions are a XOR operation. The remainder of this division should always be g or fewer bits long. The last step is to subtract the remainder to the string correspondent to $x^g M(x)$. Once again using modulo 2 resulting in the checksummed frame with polynomial $T(x)$, that will be transmitted. When the frame arrives at the receiver, it is divided by the generator polynomial. If there is a remainder, it means a transmission error occurred.

3.1.1.3 Coding scheme

In telecommunication networks, wired connections display trifling error rates when compared to wireless networks. In wireless environments transmission errors often observed and degrade the system's performance. There are two main approaches to deal with this problem, error-correcting codes and error-detecting codes [71]. Both center around the addition of redundant information to the transmitted data packet. The distinction resides in the quantity of added data. The former adds enough information to empower the receiver with the ability to deduce what the transmitted data must have been, while the later, includes only enough information to enable the receiver to detect that an error has occurred and correct it by requesting a retransmission. Typically on highly reliable channels, error-detection codes are the cheaper solution to deal with the occasional transmission error. This scheme causes a smaller increase in packet payload compared to its counterpart, even if it relies on the retransmission of data, errors are rare enough that the overall number of sent bytes will still be lower. On the other end, the fact that wireless links suffer from error rates that are orders of magnitude larger mean that retransmissions are as likely to be damaged as the original sent package. Thus, even at the cost of a bigger payload, it is much more efficient to allow the receiver to correct errors. The use of error-correcting codes is referred to as forward error correction (FEC) [71].

Naturally, LoRa uses a error-correcting code scheme, formally known as a Hamming Code [41]. This approach relies on a measure titled Hamming distance, which is essentially a metric used to denote the distance between two same length strings. Hamming Codes are a linear block code algorithm, which means that the aggregation of check and data bits is done through the use of a dictionary of codewords. A block has a length of n bits, being

n the sum of m data bits and r check bits. Essentially, before transmitting, each m bit sequence is replaced with its corresponding n length codeword, forming a block. On the receiver end, upon message arrival the reverse happens. If a decoder finds a codeword that does not exist in its dictionary, by comparing the Hamming distance between the received codeword with all of the dictionary entries one of two things can happen. Either it can safely assume that the correct codeword is the one with the smallest hamming distance, or, in the case of the smallest Hamming distance being shared between several dictionary codewords and the received damaged codeword, the receiver will ask the transmitter to retransmit this portion of data. The code rate, showed in (2.3), refers to the portion of meaningful information in a codeword or $\frac{m}{n}$ [71]. Therefore, LoRa has $m = 4$ data bits and check bits are represented by CR, which can assume a value between 1 and 4. Consequently codewords will have a length from 5 to 8 bits.



(a) Code Rate = $\frac{4}{5}$

(b) Code Rate = $\frac{4}{6}$

(c) Code Rate = $\frac{4}{7}$

(d) Code Rate = $\frac{4}{8}$

Figure 3.1: Payload symbol number increase introduced by block coding.

Error correction and detection capabilities of a Block Code are dependent on the minimum Hamming distance between codewords. To detect x errors, this distance has to be $x + 1$. To correct x errors, it has to be $2x + 1$. From [41], if assumed that blocks are defined such that the minimum Hamming distance is 1, 2, 3 and 4 for Code Rates 4/5, 4/6, 4/7 and 4/8, respectively, LoRa's error correction and detection capabilities will be as shown in Table 3.1. As evidenced in the Table, error correction will only be present in Code Rates 4/7 and 4/8, neither are capable of correcting more than one bit. Using Code Rate of 4/5 grants no benefits compared to no coding, only increases payload. Code Rate 4/6 introduces error detection of one bit, value that increases by one with every iteration

of the remaining Code Rates. Figure 3.1 shows the payload symbol number increase when block coding is introduced, using error correction on a transmission implies data sizes increase by at least 75% over the uncoded data. The curves plotted in the figure were computed using (3.7), presented in Subsection 3.1.3.

Code Rate	Error Correction (bits)	Error Detection (bits)
4/5	0	0
4/6	0	1
4/7	1	2
4/8	1	3

Table 3.1: LoRa error detecting and correcting capabilities [41].

3.1.1.4 Interleaving

Interleaving is the process of scrambling the data of a packet in order to make its transmission more resilient against burst errors. Essentially check bits are computed over the data in a different order than the order of data transmission.

In the eventuality of a interferer unhinging the transmission, a full symbol can arrive at the receiver in error, i.e. none of the demodulated bits are reliable. Being a low power wide area network specification, LoRa has a low data rate, thus it is likely that the time on air of a packet is greater then the duration of an interference. Therefore, the de-interleaving process will make so that these errors will be scattered between several symbols. This essentially increases the chances of burst errors becoming single bit errors, which can possibly be corrected by FEC.

According to the European patent [55] LoRa employs a diagonal interleaver. However, through reverse engineering the study [32] found that in reality the interleaver implemented in the LoRa standard is a diagonal interleaver with the two most significant bits reversed.

3.1.1.5 Gray Indexing

Gray Code is a binary numeral system where two successive values differ in only one bit, like evidenced in Table 3.2. In a transmission there is a limited number of possible symbols, assuming the majority of errors will be between adjacent symbols [55], i.e. symbol two can only be mistaken by symbols one and three, introducing Grey Indexing means a block of SF bits will be mapped into one of the M symbols in the constellation, where adjacent ones will be one bit shift away from each other, ensuring that the majority of errors are single bit.

Decimal	Binary	Gray Code
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110

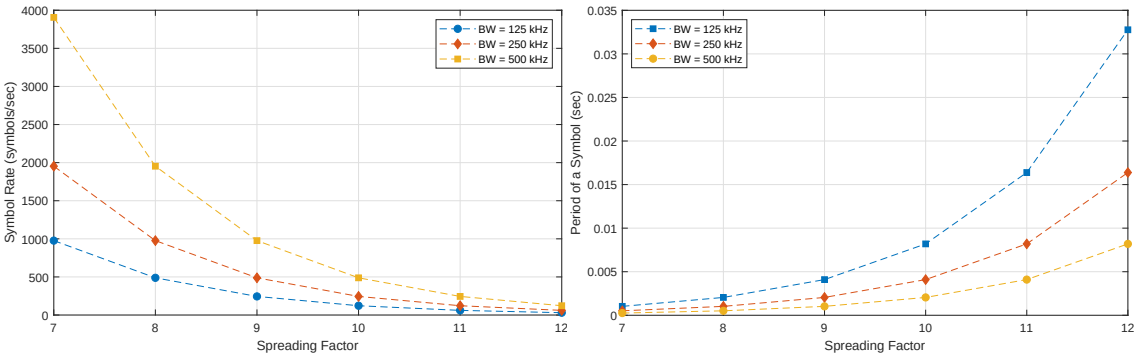
Table 3.2: Binary to Gray Coding conversion example.

3.1.2 Spreading Factor

As described in subsection 2.5.3, Lora's spreading factor affects bit rate as well as the transmission range. This parameter represents the number of encoded bits in a symbol, such that each symbol carries 2^{SF} chips and SF bits of information (3.1). Thus a symbol can carry from a minimum of 7 bits, to a maximum of 12 bits. This increment in the number of chips inside a symbol doubles its period (T_s), as evidenced in (3.2) and Figure 3.2, therefore doubling the time on air of a transmission.

$$chips\ \ per\ \ symbol = \frac{R_c}{R_s} = 2^{SF} \tag{3.1}$$

$$T_s = \frac{1}{R_s} = \frac{BW}{2^{SF}} \tag{3.2}$$



(a) Number of symbols per second.

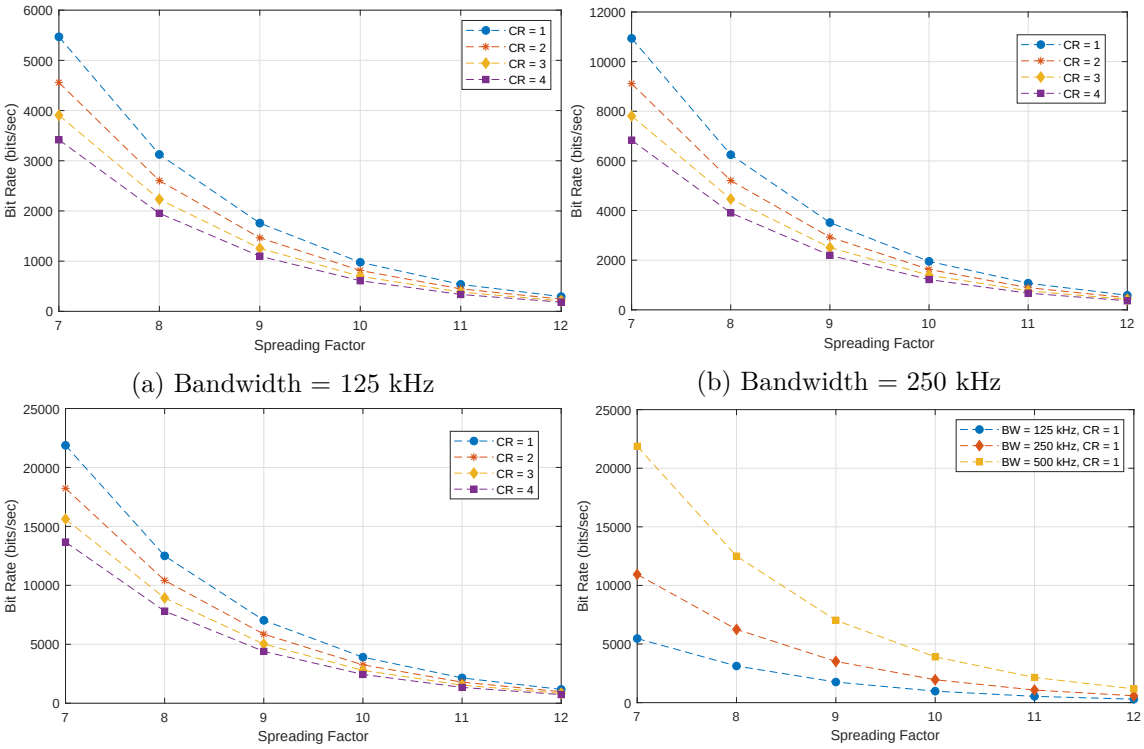
(b) Period of a symbol.

Figure 3.2: (a) Symbol rate halves with every iteration of Spreading Factor. (b) Period doubles.

The bit rate nominal value is given by (2.2). This value is inversely proportional to both the spreading factor and Code Rate used (Figure 3.3). Code Rate influence in bit rate (depicted in Table 3.3) is not a literal decrease in the overall amount of data transmitted, instead it represents the decrease in meaningful data transmitted caused by the increase of redundant information on each block. Conversely, increasing the bandwidth effectively doubles the bit rate, as shown in Table 3.4.

Spreading Factor	Coding Rate			
	1	2	3	4
7	5469	4557	3906	3418
8	3125	2604	2232	1953
9	1758	1465	1256	1099
10	977	814	698	610
11	537	448	384	336
12	293	244	209	183

Table 3.3: Coding Rate influence on bit rate with a bandwidth of 125 kHz.



(a) Bandwidth = 125 kHz

(b) Bandwidth = 250 kHz

(c) Bandwidth = 500 kHz

(d) Bit Rate comparison

Figure 3.3: Payload symbol number increase introduced by block coding.

Spreading Factor	Bandwidth (kHz)		
	125	250	500
7	5469	10938	21875
8	3125	6250	12500
9	1758	3516	7031
10	977	1953	3906
11	537	1074	2148
12	293	586	1172

Table 3.4: Bandwidth influence on bit rate with a code rate of $\frac{4}{5}$.

3.1.2.1 Orthogonality of the Spreading Factors

Lora's spreading factor are quasi-orthogonal. Theoretically this characteristic should allow receivers to detect packets using a spreading factor x whether or not they overlap in time with other transmissions employing a SF y, providing x and y are not equal. Furthermore, this detection is only possible given that the Signal to Interference plus Noise Ratio (SNIR) of the received packet exceeds a determined threshold dependent on both x and y [41]. Taking advantage of different spreading factors ought to enable an higher data flow compared to traditional modulation schemes.

3.1.2.2 Processing Gain

Processing gain (G_p) is an unique propriety of Spread Spectrum signals. Spread spectrum waveforms are modulated twice. Firstly using a traditional modulation technique, like FSK, then subsequently using a wideband modulation, Frequency Hoping (FH), Direct Sequence (DS) or Hybrid (FHDS)[17].

$$G_p = 10 \log_{10} \left(\frac{R_c}{R_b} \right) \quad (dB) \tag{3.3}$$

LoRa spread spectrum is an improved version of Direct Sequence Spread Spectrum (DSSS) modulation designed for low-cost, low-power systems [57]. In a DS system random data with a rate of R_b is multiplied by a random noise like signal called pseudorandom (PN) binary waveform with a far greater rate, achieving frequency spreading. The PN source outputs chips at a constant rate R_c, which is always bigger then the bit rate. The ratio between these two values constitutes the G_p [57], and the higher it is, the more resilient the signal becomes against interference [17]. As previously mentioned, spreading factor has an effect on bit rate which in turn affects processing gain (3.3). Therefore, increasing spreading factor grants a signal improved interference immunity, thus improving its range. Furthermore, assuming a constant data rate, increasing the bandwidth (2.6) has the same effect.

3.1.3 Time on Air

According to Semtech [56], the time on air of a packet can be determined by

$$T_{packet} = T_{preamble} + T_{payload} \,, \tag{3.4}$$

where $T_{preamble}$, as its name suggests, represents the time it takes to transmit the preamble of packet, $T_{payload}$ is the time necessary to transmit actual data. These two parameters are given by:

$$T_{preamble} = (n_{preamble} + 4,25) T_s \,, \tag{3.5}$$

$$T_{payload} = payloadSymbNb \cdot T_s \,, \tag{3.6}$$

where $n_{preamble}$ is the number of programmed preamble symbols. This parameter is configurable, an higher number of preamble symbols increases the chances that an incoming packet is detected by a receiver at the expense of air time. T_s is the period of a symbol (3.2), mentioned in subsection 3.1.2. The number of symbols in the payload, see (3.7), involves a more complex calculation since it contains several parameters:

$$payloadSymbNb = 8 + max\left(ceil\left(\frac{8PL - 4SF + 28 + 16CRC - 20H}{4(SF - 2DE)}\right) \cdot (CR + 4), 0\right) \tag{3.7}$$

where,

PL is the number of payload bytes;

CRC equal to 1 if CRC is enabled, 0 otherwise;

H has a value of 0 when the explicit header is enabled or 1 otherwise;

DE has a value of 1 when low data rate optimization is enabled or 0 if disabled.

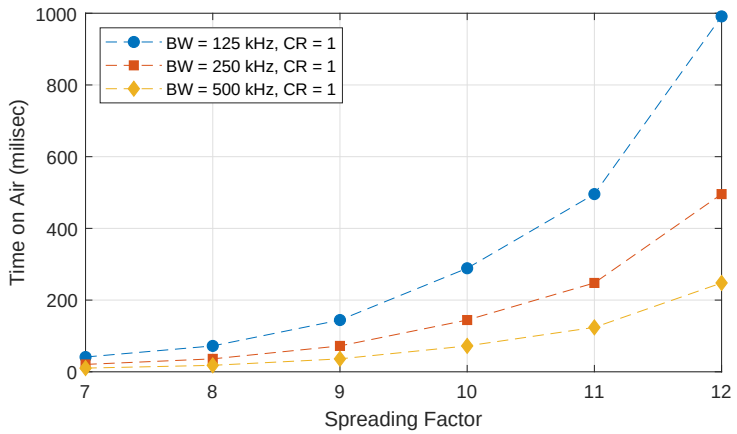


Figure 3.4: Spreading factor effect in transmission time.

3.2 LoraWan

3.2.1 Topology

In Subsection 2.5.3 it was ascertained that LoRaWAN networks are arranged in a star formation, more specifically in a star of stars formation. End-devices send messages with the assumption that it will reach at least one gateway, that in turn will relay it to a centralized network server (NS). Accordingly, the centralized system is most intelligent component of the network. It is in charge of filtering duplicate messages along side with selecting suitable gateways through which it can send DL messages to specific EDs. Additionally it monitors EDs and GWs, aggregates and forwards incoming messages to

the corresponding application server and buffers downlink messages until the intended end-device is available [8]. Gateways are a single hop away from devices and essentially act as a bridge to the NS, converting radio frequency packets into IP packets in UL and vice versa in DL communication [35]. End-devices, gateways and network server protocol stacks can be seen in Figure 3.5.

This topology has the inherent advantage of not requiring end-devices to employ routing algorithms or have listen and forward incoming messages, which makes the network entities simpler and more energy efficient. In the eventuality of a gateway failure, the centralized server most likely will lose the connection to several EDs. The lack of re-routing capabilities dictates that there is no way for these end-devices to become online until the gateway goes back up again.

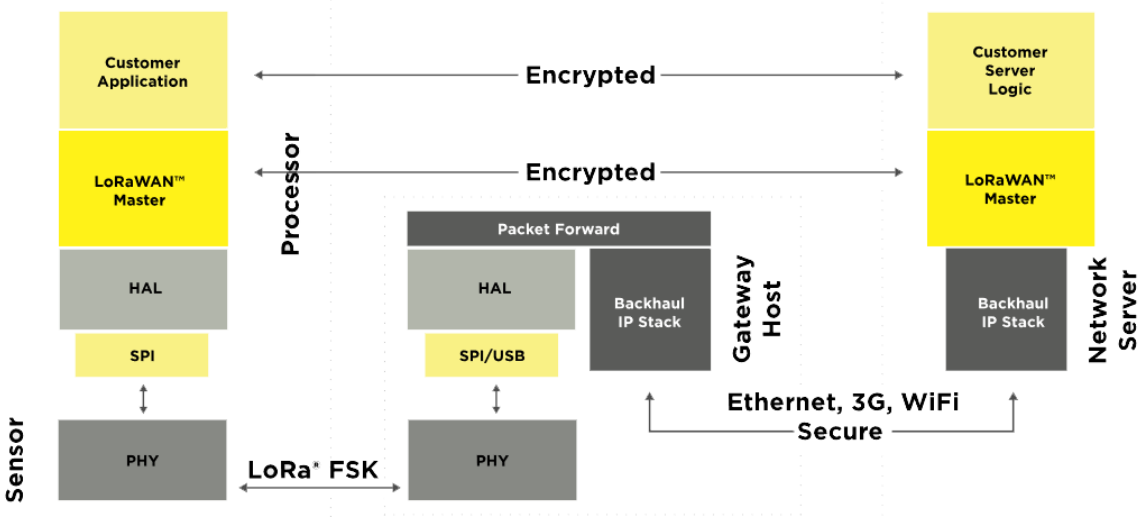


Figure 3.5: Protocol stack of LoRaWAN network components [35].

3.2.2 Encryption

Whenever a data frame carries a payload, it has to be encrypted. LoRaWAN uses an encryption scheme, based on an algorithm adopted in the IEEE 802.15.4 standard, that employs AES (Table 2.4) with a key length of 128 bits [67]. As default, the encryption and decryption processes are handled by this layer. However, LoRaWAN allows it to be done by upper layers except if the selected port is the one reserved for MAC commands (see Table 3.7). The key used by the AES procedure will be generated using either an application session key or a general network session key, if a message refers to the aforementioned reserved port. Additionally, LoRaWAN also employs a message integrity code (MIC) to prevent data tampering attacks.

3.3 Message Formats in Class A Devices

3.3.1 PHY Message Formats

LoRa has a distinguished format for uplink and downlink messages. Uplink messages are sent by end-devices to the network server through one or more gateway nodes, while downlink messages are sent by the network through one gateway to a single end-device. Both types displayed in Figures 3.6 and 3.7 use the radio packet explicit mode which in LoRa corresponds to the PHDR and PHDR_CRC fields. Explicid mode, mentioned in subsection 3.1.3 implies that an header containing payload length, CR parameter value and, exclusively in PL messages, CRC presence is appended to the message. In DL messages there is no CRC, i.e., they like payload integrity check. This is done to guarantee that the messages are as short as possible, thus minimizing their impact on duty-cycle limitations imposed on the corresponding ISM frequency band [8].

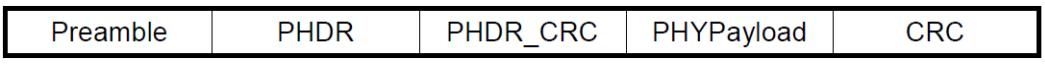


Figure 3.6: Uplink PHY message structure [67].

Figure 3.7: Downlink PHY message structure [67].

3.3.2 MAC Message Formats

(a) PHY payload structure

(b) MAC payload structure

(c) FHDR structure

Figure 3.8: Packet structure of LoRaWAN message [67].

All LoRa messages, both uplink and downlink, contain a PHYPayload (Figure 3.8a) field. The MAC header (MHDR) holds information regarding which version of the LoRa standard is being used by the device, as well as the type of message (MType) that is being sent. Messages types (Table 3.5) can be divided into three categories: joint, data and Proprietary messages.

MType	Description
000	Join Request
001	Join Accept
010	Unconfirmed Data Up
011	Unconfirmed Data Down
100	Confirmed Data Up
101	Confirmed Data Down
110	RFU
111	Proprietary

Table 3.5: MAC message types [67].

3.3.2.1 Joint Messages

These are used when an end-device attempts to joint a network. From a device point of view the joint procedure, also know as activation, compromises two exchanges with a server, a request and an accept. As might be expected, this procedure is always initiated by an end-device with an joint request message. It contains the application identifier (AppEUI), the end-device identifier (DevEUI) and a random value called DevNonce. This value is stored in the server to keep track of the network devices. Furthermore, if a request arrives with a registered DevNonce value it is ignored. When an ED is deemed worthy of joining the network, the server sends it a joint accept message. Conversely, the request message is ignored. The accept message holds another AppNonce value, that will be used by the receiver to generate an application and a network session key, a network identifier, a delay value (RxDelay) that specifies the time a receiver will have to wait for a response after transmitting, and finally a region specific list of channel frequencies.

Stored Data	Description
DevAddr	32 bit identifier of the end-device within the network, its essentially its address, similarly to an IP address in a TCP/IP network.
AppEUI	Global and unique application ID in the IEEE EUI64 address space.
NwkSkey	End-device specific network session key, used to encrypt and decrypt the payload of MAC only messages, as well as to verify data integrity.
AppSkey	End-device specific application session key, used to encrypt and decrypt the payload of application messages, as well as to verify data integrity.

Table 3.6: Data stored in an end-device after activation [67].

When the activation process is completed, the end device will have stored the values displayed in Table 3.6. In consideration of the foregoing, LoRa allows a personalized activation. The values mentioned above can be coded directly into the device enabling it to bypass the activation and participate in the network. The former procedure is known as

Over-The-Air-Activation (OTAA), while the latter is called Activation by Personalization (ABP).

3.3.2.2 Proprietary Messages

Proprietary messages are used to implement non-standard message formats that are not inter-operable with standard messages. These can only be used for communication between devices that have a clear understanding of the proprietary format specifications.

3.3.2.3 Data Messages

Data messages are used to transmit MAC commands and application data, these can be combined in a single message. Confirmed-data messages have to be acknowledged by the receiver, whereas unconfirmed data messages do not require any kind of confirmation.

The MAC payload of data messages, showed in Figure 3.8b, contains a frame header (FHDR) followed by two optional fields, a port field (FPort) and a frame payload (FRM-Payload). Whenever this payload field contains information, the frame must contain a FPort value (see Table 3.7).

Port Identifier	Description
0x00	Port reserved for MAC commands (indicates that the payload only contains MAC commands).
0x01 ... 0xDF	Application specific ports.
0xE0 ... 0xFF	Ports reserved for future standarized application extensions.

Table 3.7: FPort field values [67].

The frame header (Figure 3.8c) holds the device address, a frame control field (FCtrl), a frame counter field (FCnt) and finally a frame options field (FOpts) used to transport MAC commands. This FCtrl frame (Figure 3.9) is very important, as it is responsible for the following control operations:

- **ADR** - As previously established LoRa offers several options of data rate. LoRaWAN has an Adaptive Data Rate (ADR) setting that, if enabled, allows the network to automatically change a device data rate through the use of MAC commands. This action is triggered as an optimization attempt, the ADR algorithm my opt to increase a device SF whose SNR threshold is too low or decrease it if messages consistently arrive above the receiver sensitivity. When disabled the network will not control end-devices data rate, even if the received signal strength indicator (RSSI) is low. ADR is specially useful for managing mobile end-devices.

- **ADRACKReq** - Each time a device performs an uplink communication, it increases the frame counter field, as well as an ADR acknowledgment counter. When the later counter reaches a set limit, the device sets this field to request an ADR acknowledgment.

- **ACK** - When receiving a confirmed data message, a receiver has to respond with a data frame in which this field is set. If the sender is gateway, the end-device can acknowledge the message arrival whenever it sees fit, otherwise the acknowledgment is sent using one of the receive windows opened by the ED. Furthermore, acknowledge messages are never retransmitted and only sent as a response to the latest message received.
- **FPending** - This field signifies that the gateway has more information to send, thus is used exclusively in downlink communication.
- **FOptsLen** - Holds the length of the MAC command.

Bit#	7	6	5	4	[3..0]
FCtrl bits	ADR	ADRACKReq	ACK	FPending	FOptsLen

(a) Downlink FCtrl

Bit#	7	6	5	4	[3..0]
FCtrl bits	ADR	ADRACKReq	ACK	RFU	FOptsLen

(b) Uplink FCtrl

Figure 3.9: Frame control field contents [67].

Akin to the two distinct message formats defined in LoRa, each end-device has two frame counters. An uplink frame counter (FCntUp), increased by itself to keep track of data frames sent to the server and a downlink counter (FCntDown) sent and incremented by the NS. Every time an activation process finishes, both counters are reseted to 0. Hereafter, on each transmission an end-device will increase its UL counter when a message is sent and receive the corresponding DL counter value in the gateway response. These values should be kept in sync, meaning that every message sent was met with a response, but for control purposes, the received side stores a value that represents the max acceptable gap between them. Should the difference be greater than this gap, the receiver will deem that too many data frames have been lost and discard subsequent packets.

Several MAC commands can be exchanged between EDs and the NS. These can be piggybacked in the payload or sent in the FOpts fields, yet cannot be simultaneously present in both, and warrant the following capabilities:

- **Link Checking** - EDs can ask the NS its link margin. The reply contains the power received at the gateway.
- **ADR** - NS can request the EDs to change data rates, transmit power, repetion rate or channel through these commands.
- **Duty Cycle** - Used by the NS to set an ED aggregated duty cycle (3.8).
- **RX** - NS can set the EDs reception slot parameters and timing.

- **New Channel** - Used by NS to create new channels or request a channel change.
- **Device Status** - Network servers can request a ED status, namely, its battery level and demodulation margin.
- **Proprietary** - LoRa offers 128 MAC command identifiers reserved for proprietary network command extensions.

As expected, whenever an entity receives a MAC command requesting an action, it has to send back an acknowledge to the corresponding transmitter.

$$aggregated\ duty\ cycle = \frac{1}{2^{MaxDCycle}} \tag{3.8}$$

3.4 EU 863-870 MHz ISM Band

The 863-870 MHz band is recognized by the European Conference of Postal and Telecommunications Administrations (CEPT) as a license exempt operation band designated for a wide range specific and short range non-specific devices. Several sub-bands have been defined for specific applications, by the European Radio-communications Committee (ERC), with different operational and technical limitations. The three main subs bands segments are low band (863-865 MHz), mid band (865-868 MHz) and high band (868-870 MHz). To minimize the risk of harmful interference these sub-bands are further divided and regulated [2], as shown in Figure 3.10.

Upon approval, the European limitations are then transposed into national regulations and managed by the corresponding national administration.

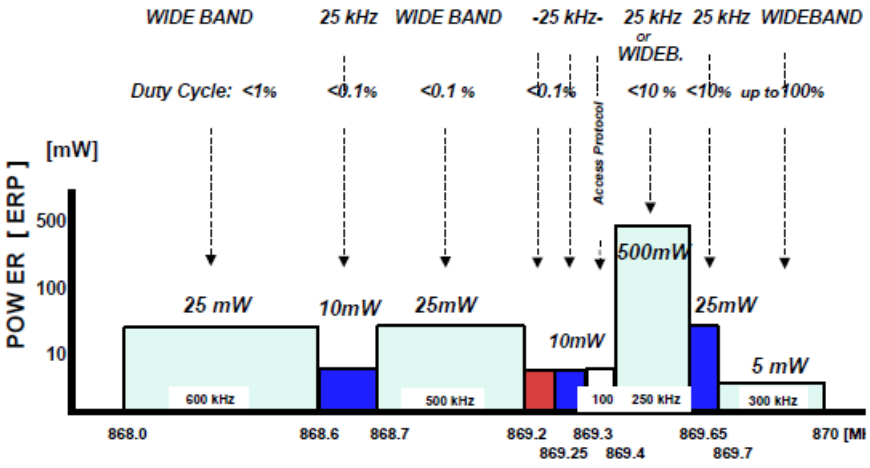


Figure 3.10: Sub divisions of the 868-870 MHz sub-band [2].

3.4.1 Regulatory Limitations

The LoRaWAN specification operates in the ISM bands, more specifically in the 868-870 MHz sub band. According to ETSI regulations, devices operating in these frequency bands are required to either employ a listen before talk model or a respect a certain duty cycle [16]. LoRaWAN adopts the latter policy [67]. Furthermore, ETSI regulations also impose a maximum permissible radiated power[16].

3.4.1.1 Effective Radiated Power (ERP)

ETSI regulates the emissions radiated by a device using the IEEE standardized definition, know as effective radiated power (3.10). ERP is the total power radiated that would have to emitted by a half-wave dipole antenna, so that it matches the actual radiated power on the source, at a distant receiver located in the direction of the antennas maximum field strength (main lobe). In essence, it measures the power emitted by a transmitter combined with the antenna ability to direct power in a given direction.

$$ERP_{dBm} = EIRP_{dBm} - 2.15. \tag{3.9}$$

EIRP or effective isotropic radiated power is identical to the ERP, with the sole exception that it uses an hypothetical isotropic antenna. Hence, (3.10) is derived from the fact that half-wave dipole antennas have a gain of 1.64 Watts or 2.15 dBs compared to an isotropic radiator, whose gain is unity, i.e. 0 dBi. In the eventuality that a device does not include an integrated antenna, the vendor is required to specify the maximum gain of an antenna that can be connected, so that the power transmitted at the device connector plus the antenna gain comply with the imposed regulations. EIRP can be written as

$$EIRP_{dBm} = 10log\left(\frac{(E^2) * (r^2)}{0.03}\right) \tag{3.10}$$

where:

r is the distance to the transmitter;

E is electrical field strength at a r distance from the transmitter.

Given that LoRa devices may operate at the channels located at the 868.1, 868.3 and 868.5 MHz band, their power is limited to a maximum of 25 mW [16, pp.29], which matches the stated default radiated transmit output power of 14 dBm in LoRaWAN specifications [67].

3.4.1.2 Duty Cycle

ETSI defines duty cycle as the ratio, expressed as a percentage, of the maximum transmitter "on"time monitored over one hour, relative to a one hour period [16, pp.41]. As previously mentioned, LoRa devices do not have listen before talk (LBT) capabilities, thus have an

imposed duty cycle of 1%. This means that each device has an air time of 36 seconds every hour.

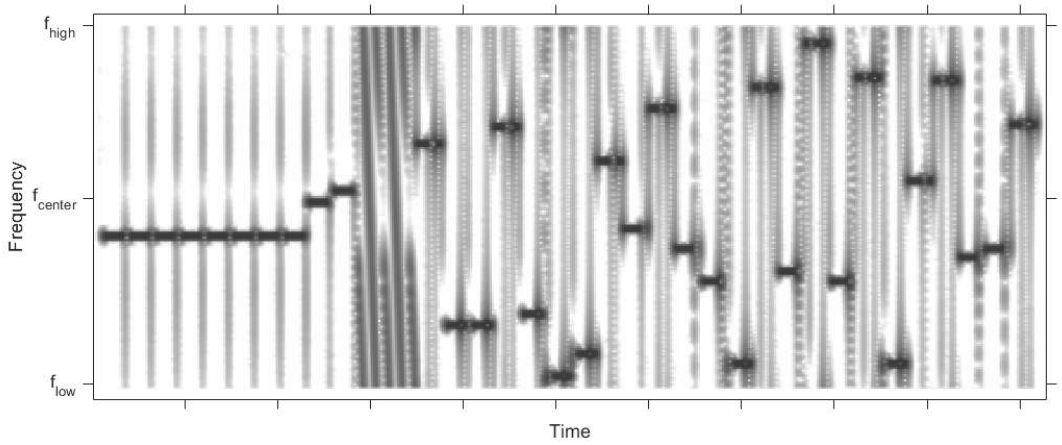
Currently, LoRaWAN specification enforces a per sub-band duty cycle limitation [67]. Each time a frame is transmitted in a given sub-band, the transmission starting time and ToA of the frame are registered. Subsequent the transmitter device cannot use the corresponding sub-band during $Toff$ seconds, which is given by (3.11), (e.g. a device that transmits a 1 second frame, will lock the used sub-band for the following 99 seconds).

$$Toff_{sub-band} = \frac{ToA}{Duty\ Cycle_{subband}} - ToA. \tag{3.11}$$

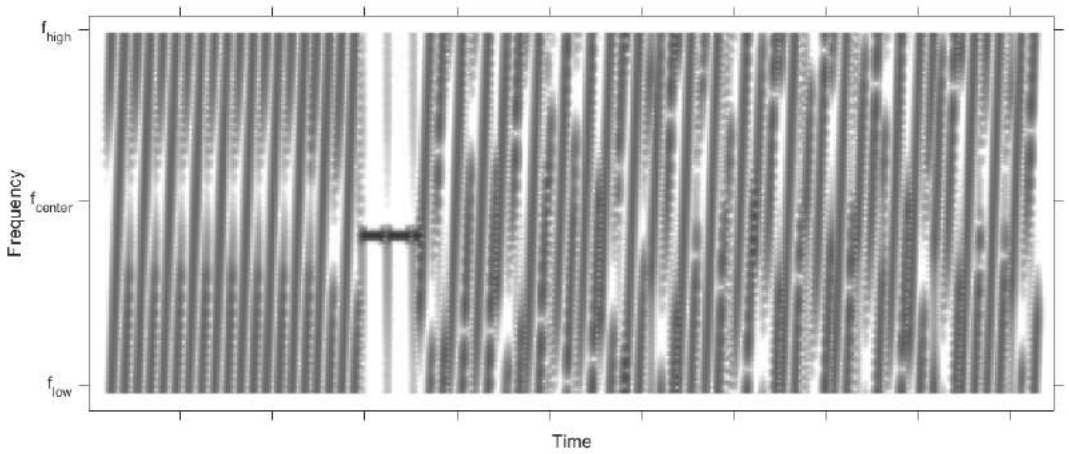
During this unavailability time, the device can still communicate in other sub-bands (channel hoping). If all sub-bands are locked behind this waiting time, it has to wait before proceeding with the frame transmission [67].

3.4.2 Preamble Format

LoRa's preamble is represented by a set of symbols containing only identical up-chirps (Figure 3.11a). Once de-chirped and applied the Fast Fourier Transform (FFT), a receiver is able to identify a signals preamble if enough consecutive FFTs have the same maximum peak value. The two down-chirps symbols (Figure 3.11a) that follow are known as the start of the frame delimiter. These are synchronization symbols used for time synchronization. LoRa's specifications define a preamble of eight symbols and the sync word 0x34 in the 863-870 MHz band [67].



(a) Up-chirps (preamble and body)



(a) Down-chirps (start of frame delimiter)

Figure 3.11: De-chirped LoRa signal [32].

CHAPTER 4

Theoretical LoRa Performance

4.1 Uplink PHY Performance Model

The study [23] proposes an approach to measure the theoretical uplink performance of a LoRa network containing a single gateway. The model considers a link outage condition revolving around a signal to noise ratio threshold value that represents the minimum SNR value above which a frame can be successfully decoded. Suppose a LoRa signal $s(t)$ is transmitted over a Rayleigh distributed flat fading channel $h(t)$. It is possible to determine the probability of a node transmission outage caused by path loss, shadowing and fading. The channel $h(t)$ is modeled as a complex zero-mean independent Gaussian random variable (RV) with unit variance, namely Rayleigh fading.

Path loss (4.2) denotes the decrease in power density of a electromagnetic wave traveling through space, and can be derived from Friis free space equation [40], represented below as

$$\frac{P_R}{P_T} = G_R \cdot G_T \cdot \frac{1}{L} \cdot \left(\frac{\lambda}{4\pi d}\right)^2 , \tag{4.1}$$

$$g(d) = 10\log_{10}\left(\frac{P_T}{P_R}\right)^{\alpha} = -10\log_{10}\left(\frac{G_R G_T \lambda^2}{(4\pi)^2 d^2 L}\right)^{\alpha} \quad (dB) , \tag{4.2}$$

where P_R and P_T represent the received and transmitted power, respectively, G_R and G_T are the gains of the receiver and transmitter antennas, L denotes system loss factors like transmission line attenuations and antenna losses, λ is the carrier frequency wavelength and d is the euclidean distance between receiver and transmitter. The mathematical formulation accurately characterizes the attenuation over distance experienced by electromagnetic waves propagating in free space. However, it does not account for the sheer diversity of real world environments that dissimilarly affect propagation [40]. Hence, the decay of

the received power will vary accordingly to the path traveled from the transmitter to the receiver. The path loss exponent, α expresses the environment respective rate of decay (Table 4.1) thus allowing a more accurate representation of these phenomena. Additionally, (4.1), ergo (4.2), are only valid for values of d corresponding to the far-field region of the transmitter antennas, i.e. $d >> \lambda$ [40]. The path loss equation can be further simplified by assuming that both the transmitter and receiver antennas are isotropic, i.e. have unity gain.

Environment	**Path Loss Exponent(α)**
Free Space	2
Urban	2.7 - 3.5
Shadowed urban	3 - 5
In building line-of-sight	1.6 - 1.8
In building obstructed	4 - 6
In factory obstructed	2 - 3

Table 4.1: Path loss exponent in different environments [40]

Shadowing is caused by objects obstructing the wave propagation path, and is characterized by power fluctuations on the received signal. The effect of this phenomenon is represented in this model as additive white Gaussian noise (AWGN), which follows a Rayleigh distribution with mean one and variance (4.3) equal to the sum of the noise floor (4.4) at room temperature, plus the device specific noise figure (NF). According to [57], the noise figure of the hardware considered is 6 db, and this value will be assumed in what follows being defined as

$$\sigma^2 = Noise\ \ Floor + NF \quad (dBm) \tag{4.3}$$

$$Noise\ \ Floor = 10\log_{10}(k_B \cdot T \cdot BW \cdot 1000) \quad (dBm) \tag{4.4}$$

where:

k_B = Boltzmann's Constant ($\approx 1.38 \cdot 10^{-23}$);

T = Temperature in Kelvins (room temperature is approximately $293k$);

BW = channel bandwidth in Hertz;

Given that LoRa offers a scalable bandwidth, the noise floor value will vary accordingly. Table 4.2 contains the values obtained using (4.4).

Finally, the probability of outage in the Rayleigh channel caused by fading should include the effect of path loss and shadowing on the signal to noise ratio (4.5), given by

$$SNR = \frac{P \cdot g(d) \cdot |h|^2}{\sigma^2}\,, \tag{4.5}$$

where P is the end-device transmission power, which according to ETSI regulations is limited to 14 dBm, $|h|^2$ is the aforementioned channel gain modeled as a exponential RV with unity average.

Bandwidth (kHz)	Noise Floor (dBm)
125	-122.961
250	-119.951
500	-116.941

Table 4.2: Noise floor values for all bandwidths.

Sensitivity (S) is the metric that denotes how a faint an input signal can be in order to be successfully received. Naturally, the SNR threshold, represented by b, is dependent on the receiver sensitivity as observable in (4.6), extracted from [56].

$$S = -174 + 10 \cdot log_{10}BW + NF + b \;\; (dBm)\,, \tag{4.6}$$

Since S values are fixed and a function of spreading factor, (4.6) can be rearranged as $b = S - \sigma^2$, where σ^2 is given by (4.3) and the SF specific sensitivity values are given in [57].

Bandwidth (kHz)	Spreading Factor	Sensitivity (dBm)	b (dBm)
125	7	-123	-6
	8	-126	-9
	9	-129	-12
	10	-132	-15
	11	-134.5	-17.5
	12	-137	-20

Table 4.3: Receiver sensitivity and SNR threshold for different spreading factors with a bandwidth of 125 kHz and code rate of one.

A device transmission wont be successful, that is, the packet will not be successful decoded if the SNR received is lower then the threshold values given in table 4.3, thus the coverage probability is given by the complement to the outage probability (4.7).

$$\begin{aligned} P[SNR \geq b] &= P\left[\frac{P \cdot g(d) \cdot |h|^2}{\sigma^2} \geq b\right] = \\ &= exp\left(\frac{\sigma^2 \cdot b}{P \cdot g(d)}\right) \end{aligned} \tag{4.7}$$

For simulation purposes, it was defined that the network will be composed by a central gateway and several end-devices located uniformly in a radius of twelve kilometers, as seen in Figure 4.1. The network is divided into six rings, one for each SF value, i.e the devices inside a two kilometers radius from the gateway will transmit using spreading factor of 7, devices in the 2-4 km area will use SF of 8 and so on.

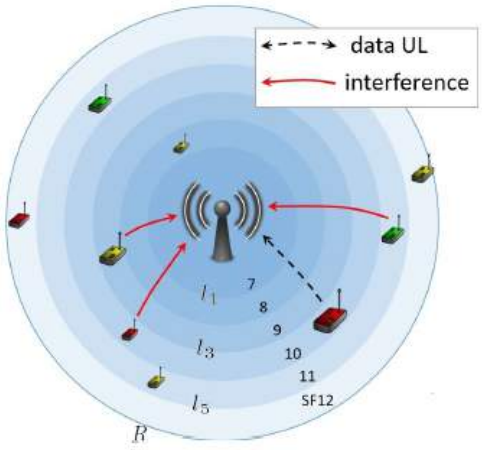
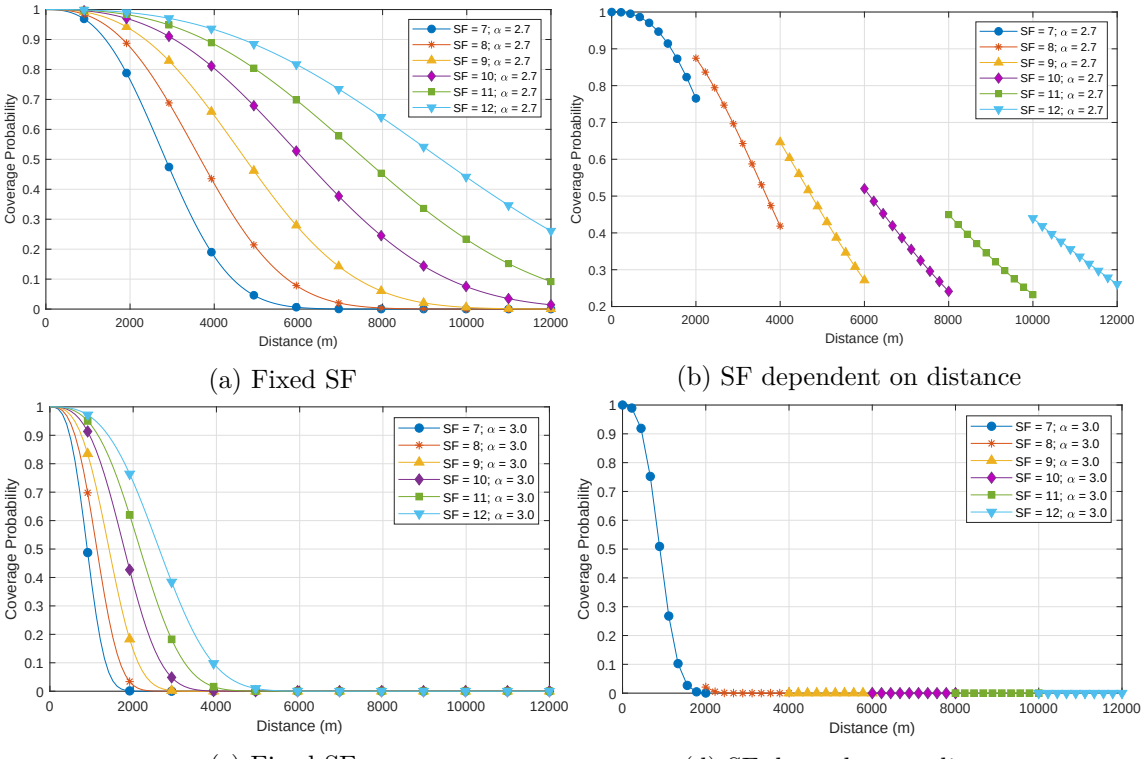


Figure 4.1: Network layout [23].

The simulation results (Figure 4.2) were obtained by varying the distance and using the corresponding SNR threshold and SF values for a bandwidth of 125 kHz. Lastly, it is assumed that the network is spread over an urban area, thus, according to Table 4.1 $\alpha = 2.7$, to emulate a favorable urban propagation environment, and $\alpha = 3$ for an harsher one.



(a) Fixed SF

(b) SF dependent on distance

(c) Fixed SF

(d) SF dependent on distance

Figure 4.2: Coverage probability.

As evidenced in Figures 4.2a and 4.2c, path loss highly impacts on the network coverage distance. Indubitably, splitting the network area into rings, each representing a different

spreading factor, will enable an higher probability of coverage while maintaining the best bit rate compromise. Conversely, adopting a single SF across the network will empower users to alternate between scenarios favoring maximum bit rate while sacrificing distance or vice versa, depending on the intended application. Nevertheless, environments with highly adverse propagation conditions will take a toll on the achievable coverage distance of a LoRa network, regardless of the SF or BW used in the transmissions.

4.2 PHY/MAC Uplink Performance of Class A LoRa Networks

As a consequence of the Aloha like behavior of Class A LoRa devices, frame collision in such a network is inherent and bound to happen. LoRa, being an iteration of DSSS modulation, takes advantage of its frequency diversity to recover information from weak signals [24], meaning when a frame is involved in a collision, under certain conditions, it can still be decoded by a LoRa receiver. This is against the traditional collision model, where all frames involved in a collision are considered lost [24]. As mentioned in Subsection 3.1.2.1, LoRa spreading factors are quasi-orthogonal, as a result the interference affecting each signal is not exclusively caused by the concurrent same SF transmissions. Rather, a transmission can be hindered by co-SF interference, that stems from concurrent transmissions in the same channel with the same SF, and inter-SF interference caused by the aforementioned imperfect orthogonality. This was addressed in [27], where it was reported that inter-SF interference can have a notable effect on link success in highly dense networks, although less prominent otherwise. Furthermore, in [24] it is observed that two devices can successfully transmit simultaneous using different spreading factors, given that none of the received signals power is significantly higher. This leads to the conclusion that co-SF interference is still by large the main cause of link outage due to interference, thus the focal point of this model. It is of importance to note that the level of power discrepancy necessary for link outage is still unclear. In [24] it is reported that a frame can be decoded if its power is at least 2 times stronger (6 dB) than a competing signal, however empirical data from [9] show this difference to be around 15 dB.

Conversely to [23], it is considered a PHY-layer SINR-based capture condition using the method presented in [20], which was adapted to suit a generic LoRa network. Thereby, it is assumed that multiple frames can be successfully received at the same time, which can be viewed as an upper bound of the PHY-layer performance. The signal to interference plus noise ratio threshold value are obtained in the same manner as in Section 4.1. For added redundancy node distribution along the network radius is done trough a stochastic spatial model considering. An uplink MAC protocol is considered, where the number of devices involved in a collision is modeled for exponential traffic sources. Lastly, the joint PHY/MAC performance is studied through the average number of successfully decoded frames for different levels of network load and physical-layer conditions.

4.2.1 Medium Access Control

As previously mentioned in Section 2.5.3, LoRaWAN is the MAC protocol designed to run on top of LoRa's modulation scheme. It provides bidirectional communications for all classes of devices. Class A devices initiate communication by sending an uplink message in a random access mode, i.e a device starts a transmission whenever it has a frame to send, akin to ALOHA protocol. If the message is successfully received, the gateway might then send a downlink response.

Considering a network composed of n end devices, where each node, independently from other nodes, continuously generates a frame at a constant average rate. This means each node will generate λ frames per unit of time with an average of λ^{-1} time units per frame. In this work it is considered that the frames inter-arrival time is exponentially distributed and its probability density function (PDF) takes the form of

$$f_I(x) = \lambda e^{-\lambda x}. \tag{4.8}$$

Because of the ALOHA like behavior of class A devices, coupled with the assumption that the probability of a node generating more than a single frame per time unit being negligible, due to LoRa devices imposed low transmission rate and duty cycle regulations referenced in Section 3.4.1, each node, per time unit, will transmit a frame with probability

$$\tau = \begin{cases} \lambda, & 0 \leq \lambda \leq 1 \\ 1, & \lambda > 1. \end{cases}$$

As a result of the frames inter-arrival time distribution, the average number of frames generated by n nodes per time unit at a rate of λ will be $n\lambda$. For this reason the number of frame transmissions per time unit can be represented by the random variable K distributed as a n truncated Poisson distribution expressed as

$$f_K(k) = \frac{e^{-n\lambda}(n\lambda)^k}{k!} \left(\sum_{m=0}^{n} \frac{(n\lambda)^m e^{-(n\lambda)}}{m!} \right)^{-1}, k = 0, ..., n. \tag{4.9}$$

On the basis of (4.9), the probability of occurring at least one transmission in a given time unit is the complement of the probability of no device transmitting, i.e. $1 - f_K(0)$. Being the number of nodes involved in a transmission the RV C, by integrating the aforementioned complementary probability into (4.9), the probability of c devices concurrently transmitting a frame in a given time unit can be written as

$$\mathrm{P}[C = c] = \frac{f_K(c)}{1 - f_K(0)}, c = 1, ..., n. \tag{4.10}$$

By observing $P[C = c]$ it is possible to verify that whenever $c > 1$, it also represents the probability of c frames being involved in a collision. Lastly, since a network of n nodes will produce an average of $n\lambda$ frames per time unit, the total load generated by the devices will be $G = n\lambda$.

4.2.2 Network Assumptions

In a similar vein to the model described above in Section 4.1, the network considered features a circular region of radius R centered at the gateway. A set of n nodes are uniformly distributed within the circumferential area $A = \pi R^2$ with spatial density $\sigma = \frac{n}{\pi R^2}$. This means that the average distance between nodes is unvarying all throughout the network, regardless of the distance to the center. Since the circumference of a circle grows linearly with its radius, a twice as long circumference will hold twice as many nodes so that the spatial density remains the same. Thence, being d_k the random variable that represents the Euclidean distance between the k-th node and the gateway, its PDF can be written as a ratio between the perimeter of the circle with radius r and the total area of the network, such that

$$f_{d_k}(r) = \begin{cases} \frac{2\pi r}{A}, & 0 \leq r \leq R \\ 0, & otherwise. \end{cases} \tag{4.11}$$

The received power from each node transmission is affected by three propagation effects, path loss, small-scale and large-scale fading. The gain due to path loss remains identical to (4.2), except it was re-rewritten as $g(d_k) = (\frac{w}{d_k+1})^{\alpha}, d_k \in [0, R]$, where w is given by $\frac{c}{4\pi f_c}$, being c the speed of light and f_c the carrier frequency. Fading is modeled as in [20], thus Rayleigh fading and Log-normal shadowing is assumed. The former, small-scale fading represents the effect of multipath propagation when there is no dominant propagation path along a line of sight between the transmitter and receiver, i.e. there are several multipath fading channels between an ED and the gateway. According to the central limit theorem the in-phase (I) and quadrature (Q) components of the received signal are independent complex Gaussian normal distributed random variables. Representing the respective signal components with the random variables X_I and X_Q,

$$X_I \ and \ X_Q \sim N(0, \sigma^2).$$

Further, the book *Microwave Mobile Communications* presents a mathematical approximation [30, pp. 13-19] and experimental results [30, pp. 65-72] demonstrating that the envelope wave of two independent and identically distributed (iid) Gaussian variables is Rayleigh distributed. Thus, denoting the small-scale fading amplitude as the RV A_ζ,

$$A_\zeta = \sqrt{X_I^2 + X_Q^2}, \ \ A_\zeta \sim Rayleigh(\sigma_\zeta).$$

Accordingly, the PDF of the received envelope signal is

$$f_{A_\zeta}(x) = \frac{x}{\sigma_\zeta^2} e^{\frac{-x^2}{2\sigma_\zeta^2}}, \tag{4.12}$$

where σ_ζ^2 is the variance of each of the aforementioned iid Gaussian RVs. Following the Rayleigh distribution relationship with the exponential distribution, i.e. if $X \sim Exponential(\lambda)$ then $Y = \sqrt{X} \sim Rayleigh\left(\frac{1}{\sqrt{2\lambda}}\right)$, its possible to conclude that the power

of the small-scale fading, which is the square of the amplitude, is exponentially distributed with PDF

$$f_{P_\zeta}(x) = \frac{1}{2\sigma_\zeta^2} e^{\frac{-x}{2\sigma_\zeta^2}}, \tag{4.13}$$

where $2\sigma_\zeta^2$ is the average gain, which is considered to be normalized gain, i.e $2\sigma_\zeta^2 = 1$. As mentioned in Section 4.1, shadowing causes power fluctuations on the received signal. This effect manifest itself over long distances, i.e. over a myriad of wavelengths. Empirical studies performed by diverse authors, e.g. Reudink and Black in 1972 and Egli in 1957, concluded that the actual received mean power of a signal randomly fluctuates with a log-normal distribution around the area-mean power [53, pp. 18-22]. Received or local mean denotes the average over approximately forty wavelengths, while area-mean is the average over tens or hundreds of meters. Log-normal means that the local mean is expressed in logarithmic values. The received power expressed in logarithmic units (Np) as the zero mean Gaussian RV P_{log} with variance σ_ξ^2 follows a normal distribution [53, pp. 21], such that

$$f_{P_{log}}(x) = \frac{1}{\sqrt{2\pi} \cdot \sigma_\xi} e^{\frac{-x}{2\sigma_\xi^2}}. \tag{4.14}$$

Since P_{log} is the natural logarithm of the local mean power (P_ξ) over the area mean power (P_A), i.e. $P_{log} = \ln \frac{P_\xi}{P_A}$, the equation can be rearranged to make the local mean power the subject thus

$$P_\xi = e^{P_{log}} \cdot P_A.$$

Considering that $P_{log} \sim N(0, \sigma_\xi^2)$ and the following log-normal distribution proprieties:

1. If $X \sim N(\mu, \sigma_\xi^2)$, then $e^X \sim LogNormal(\mu, \sigma_\xi^2)$;
2. If $Y \sim LogNormal(\mu, \sigma_\xi^2)$, then $aY \sim LogNormal(\mu + ln(a), \sigma_\xi^2)$;

It is possible to conclude that the received power (P_ξ), in Watts, is log-normal distributed as

$$P_\xi \sim LogNormal(ln(P_A), \sigma_\xi^2).$$

Therefore its PDF is given by

$$f_{P_\xi}(x) = \frac{1}{\sqrt{2\pi}\sigma_\xi x} e^{\frac{-(ln(x)-\mu_\xi)^2}{2\sigma_\xi^2}}, \tag{4.15}$$

where $\mu_\xi = ln(P_A)$ is the mean power and σ_ξ^2 is the standard deviation, both in expressed in natural units. Their values in Decibels can be obtained using $\mu_{dB} = \frac{10}{ln(10)}\mu$ and $\sigma_{\xi_{dB}} = \frac{10}{ln(10)}\sigma_\xi$ [69, pp. 98]. Moreover, $\sigma_\xi > 0$ and average gain is considered to be unity, thus $\mu_\xi = -\frac{\sigma_\xi^2}{2}$. On account of the mathematical intractability of the log-normal distribution, the large-scale fading effect will be fittingly approximated to a gamma distribution, as proposed in [1]. The n-th moment of a log-normal distributed RV X is given by:

$$E[X^n] = e^{n\mu + \frac{1}{2}n^2\sigma^2}.$$

For this reason, the first and second moments of the large-scale fading power, that respectively represent the arithmetic mean and expected square, are $E[X] = e^{\mu_\xi + \frac{\sigma_\xi^2}{2}}$ and $E[X^2] = e^{2\mu_\xi + 2\sigma_\xi^2}$. The log-normal distribution variance is given by

$$Var[X] = E[X^2] - E[X]^2,$$

such that, $Var[X] = e^{e\mu_\xi + \sigma_\xi^2}(e^{\sigma_\xi^2} - 1)$. The gamma distribution is parametrized by the shape (k) and scale (θ), with arithmetic mean $E[X] = k\theta$ and variance $Var[X] = k\theta^2$. The relation between the log-normal and gamma distribution parameters can then be obtained by matching the first moment and variance of the distributions with the subsequent system of equations:

$$\begin{cases} k\theta = e^{\mu_\xi + \frac{1}{2}\sigma_\xi^2} \\ k\theta^2 = e^{2\mu_\xi + \sigma_\xi^2}(e^{\sigma_\xi^2} - 1) \end{cases} \Leftrightarrow \quad \begin{cases} \theta = e^{\mu_\xi + \frac{\sigma_\xi^2}{2}}(e^{\sigma_\xi^2} - 1) \\ k = (e^{\sigma_\xi^2} - 1)^{-1} \end{cases}$$

Denoting the shape and scale parameters of the gamma distribution as ϑ and $\frac{\omega_s}{\vartheta}$ it can be concluded that $\vartheta = (e^{\sigma_\xi^2} - 1)^{-1}$ and $\omega_s = e^{\mu_\xi}\sqrt{\frac{\vartheta+1}{\vartheta}}$. Thus the log-normal shadowing power can be accurately represented as the gamma distribution

$$P_\xi \sim Gamma(\vartheta, \frac{\omega_s}{\vartheta}),$$

with the probability density function:

$$f_{P_\xi}(x) = \frac{1}{\Gamma(\vartheta)}\left(\frac{\vartheta}{\omega_s}\right)^{\vartheta} x^{\vartheta-1} e^{-x\frac{\vartheta}{\omega_s}}, \tag{4.16}$$

where $\Gamma(.)$ represents the Gamma function. Lastly, being Ψ_i the random variable that represents the composite effects of small and large-scale fading, the joint effect of these phenomena is given by $f_{\Psi_i}(x) \approx f_{P_\xi}(x) \cdot f_{P_\zeta}(x)$. The Rayleigh fading gain, which is exponential distributed (4.13), in conformity with the propriety that states if $X \sim Exp(\lambda)$ then $X \sim Gamma(1, \lambda^{-1})$ can be written as a Gamma distributed random variable $P_\zeta \sim Gamma(1, 2\sigma_\zeta^2)$. Therefore, the joint fading effect gain Ψ_i is distributed according to a generalized-k distribution with PDF [34]

$$f_{\Psi_i}(x) \approx \frac{2x^{\frac{\vartheta-1}{2}}}{\Gamma(\vartheta)}\left(\frac{\vartheta}{\omega_s}\right)^{\frac{\vartheta+1}{2}} K_{\vartheta-1}\left(\sqrt{\frac{4\vartheta x}{\omega_s}}\right), \tag{4.17}$$

where K is the modified Bessel function of second kind and order $\vartheta - 1$, ϑ is the shadowing parameter and ω_s is the mean power. This is known as the Gamma-Gamma model which was originally introduced to model scattering in radar systems and later widely adopted as a composite fading model in wireless communications [3]. However, alike the log-normal distribution, the generalized-k distribution puts forward analytical difficulties. To overcome these constrains, this distribution can be approximated to a gamma distribution though the use of the moment matching method, as proposed by [3]. Denoting Ψ_i as a gamma distributed RV with shape parameter k_Ψ and scale parameter θ_Ψ, then

$$\Psi_i \sim Gamma(k_\Psi, \theta_\Psi)$$

By matching the first and second moments of the gamma distribution with the generalized-k distribution, the relation between parameters can be written as

$$\begin{cases} k_\Psi \theta_\Psi = \omega_s \\ \theta_\Psi^2 k_\Psi (k_\Psi + 1) = K_1 \omega_s^2 \end{cases} \Leftrightarrow \quad \begin{cases} \theta_\Psi = (K_1 - 1)\omega_s \\ k_\Psi = \frac{1}{K_1 - 1} \end{cases},$$

where $K_1 = \frac{(\omega_n+1)(\vartheta+1)}{\omega_n \vartheta}$ and ω_n is the Nakagami multipath fading parameter, which is considered unity thus restoring the Rayleigh fading condition and consequently $K_1 = \frac{2(\vartheta+1)}{\vartheta}$. With this, it is possible to conclude that θ_Ψ and k_Ψ are given by $(\frac{2(\vartheta+1)}{\vartheta} - 1)\omega_s$ and $\frac{1}{\frac{2(\vartheta+1)}{\vartheta} - 1}$, respectively. Finally, the PDF of the Rayleigh fading and shadowing power gain is given by

$$f_{\Psi_i}(x) = \frac{x^{k_\Psi - 1}}{\Gamma(k_\Psi)\theta_\Psi^{k_\Psi}} e^{-\frac{x}{\theta_\Psi}}. \tag{4.18}$$

Regarding the noise at the gateway, it is assumed to be Additive White Gaussian noise with zero mean and variance equal to (4.3). Since the AWGN follows a complex normal distribution, the euclidean norm of its in-phase and quadrature components, i.e. the envelope, is Rayleigh distributed. As a result, the power of the AWGN is exponentially distributed, thus denoting the power as the RV N_0, then $N_0 \sim Exp(\sigma_{N_0}^2)$ with PDF

$$f_{N_0} = \sigma_{N_0}^2 e^{-x\sigma_{N_0}^2}. \tag{4.19}$$

where $\sigma_{N_0}^2$ is the variance in natural units, i.e. $\sigma_{N_0}^2 = 10^{\frac{\sigma^2}{10}}$.

4.2.3 Physical Layer

Following from Section 4.2.1, it is considered that $1 \leq n_c < n$ nodes transmit data simultaneous to the gateway. Considering that all the received signals from the competing EDs are i.i.d. random variables, the aggregate power received in the LoRa gateway is given by

$$\Xi = \sum_{k=1}^{n_c} P_k + N_0, \tag{4.20}$$

where P_k is the RV representing the power received by the gateway from the k-th LoRa device, and N_0 is the AWGN power at the gateway. As aforementioned, the received power is affected by path loss and the composite effect of shadowing and Rayleigh fading, thence

$$P_k = P_T \Psi_k (\frac{w}{d_k + 1})^\alpha, \tag{4.21}$$

where P_T is the end device transmission power (limited to 14 dBm). In this scenario it is considered that the LoRa gateway can receive multiple frames transmitted with the same Spreading Factor. On those grounds the signal to interference plus noise ratio (SINR) associated with a transmission from a generic device j is

$$\gamma_j = \frac{P_j}{\Xi - P_j}. \tag{4.22}$$

Essentially, every concurrent signal to the one transmitted by the node j is seen as inter SF interference. The successful frame capture condition is the same described in Section 4.1, from [23], i.e. a frame can be successfully decoded if its SINR value is above a Spreading Factor specific threshold b,

$$\gamma_j > b. \tag{4.23}$$

The probability of decoding an individual frame at the gateway can be derived from (4.23), which implies the following condition

$$P_j = \frac{b}{b+1}\Xi, \tag{4.24}$$

from which it is possible to conclude that the probability of outage is $P[P_j - \frac{b}{b+1}\Xi \leq 0]$. Accordingly, the probability of successfully decoding a frame given n_c concurrent transmissions can be written as the complement of the outage probability as follows

$$P[S|n_c] = 1 - P[P_j - \frac{b}{b+1}\Xi \leq 0]. \tag{4.25}$$

By considering a random variable $\Upsilon = P_j - \frac{b}{b+1}(\sum_{k=1}^{n_c} P_k + N_0)$, its characteristic function (CF) can be written as

$$\varphi_\Upsilon(t) = \varphi_{P_j}\left(\frac{t}{b+1}\right) \cdot \prod_{k=1,k\neq j}^{n_c} \varphi_{P_k}\left(-\frac{b}{b+1}t\right) \cdot \varphi_{N_0}\left(-\frac{b}{b+1}t\right), \tag{4.26}$$

where φ_{N_0} is the characteristic function of the AWGN power, φ_{P_j} represents the characteristic function of the frame power to be decoded and φ_{P_k} is the power of the interfering frames. Regarding φ_{N_0}, since the power of the AWGN is exponentially distributed, it represents the characteristic function of the Gaussian noise,

$$\varphi_{N_0}(t) = \frac{\sigma_{N_0}^2}{\sigma_{N_0}^2 + it}. \tag{4.27}$$

It is assumed that each individual power that compose P_k is independent and identically distributed, which implies that the PDF of aggregate interference power given n_c concurrent transmissions is the convolution of the PDFs of each individual interference component P_k. By definition, the characteristic function of an RV is the Fourier transforms of its PDF, thus the characteristic power of the aggregate interference power (φ_{agg}) is the multiplication of each components CF, i.e $\varphi_{agg} = \varphi_1(t) \cdot \varphi_2(t) \cdot ... \cdot \varphi_{P_k}(t) = (\varphi_{P_k}(t))^{n_c-1}$. In this way, (4.26) can be simplified as

$$\varphi_\Upsilon(t) = \varphi_{P_j}\left(\frac{t}{b+1}\right) \cdot \varphi_{N_0}\left(-\frac{b}{b+1}t\right) \cdot \left(\varphi_{P_k}\left(-\frac{b}{b+1}t\right)\right)^{n_c-1}. \tag{4.28}$$

The CF of the power received from the node k is by definition

$$\varphi_{P_k}(t) := \int_{-\infty}^{\infty} e^{itx} f_{P_k}(x)dx. \tag{4.29}$$

Taking into account (4.21), i.e. the composite fading effect and the path loss, which is dependent on the spatial distribution of the transmitters (4.11), the CF of the power received can be rewritten as

$$\varphi_{P_k}(t) = \int_0^\infty \int_0^R e^{itP_T\psi(\frac{w}{r+1})^\alpha} f_{\Psi_j}(\psi) f_{d_k}(r) d\psi dr, \tag{4.30}$$

where ψ is the composite fading parameter and r is the euclidean distance between the k-th node and the gateway. By substituting the values of $f_{\Psi_j}(\psi)$ and $f_{d_k}(r)$ into (4.30), it can be developed as

$$\begin{aligned}\varphi_{P_k}(t) &= \int_0^\infty \int_0^R e^{itP_T\psi(\frac{w}{r+1})^\alpha} \cdot \frac{\psi^{k_\Psi-1}}{\Gamma(k_\Psi)\theta_\Psi^{k_\Psi}} e^{-\frac{\psi}{\theta_\Psi}} \cdot \frac{2\pi r}{\pi R^2}\ d\psi dr \\ &= \frac{2}{\Gamma(k_\Psi)\theta_\Psi^{k_\Psi} R^2} \int_0^\infty \int_0^R e^{itP_T\psi w^\alpha (r+1)^{-\alpha}} \cdot e^{-\frac{\psi}{\theta_\Psi}} \cdot \psi^{k_\Psi-1} \cdot r\ d\psi dr \\ &= \frac{2}{\Gamma(k_\Psi)\theta_\Psi^{k_\Psi} R^2} \int_0^\infty e^{-\frac{\psi}{\theta_\Psi}} \cdot \psi^{k_\Psi-1} \cdot \varphi_{P_k}^g\ d\psi,\end{aligned} \tag{4.31}$$

such that $\varphi_{P_k}^g$ is the characteristic function representing the path loss experienced by the k-th node, given by $\int_0^R e^{itP_T\psi w^{-\alpha}(r+1)^\alpha} \cdot r\ dr$.

Lemma 1. *If $n \neq 0$ and $z = \frac{m-1}{n}$ the integral of the exponential combined with a rational function holds the following equality [50, pp. 107, eq. 2.325.6]:*

$$\int \frac{e^{ax^n}}{x^m}\ dx = \frac{(-1)^{z-1} a^z \Gamma(-z, -ax^n)}{n},$$

where $\Gamma(-z, -ax^n)$ is the incomplete Gamma function, given by $\int_{-ax^n}^\infty e^{-t} \cdot t^{-(z+1)}\ dt$ [50, pp. 899, eq. 8.350.2].

Rewriting $\varphi_{P_k}^g$ as

$$\varphi_{P_k}^g = \int_0^R e^{itP_T\psi w^\alpha (r+1)^{-\alpha}} \cdot (r+1)\ dr - \int_0^R e^{itP_T\psi w^\alpha (r+1)^{-\alpha}}\ dr, \tag{4.32}$$

it is possible to apply the equality displayed in Lemma 1, such that

$$\begin{aligned}\varphi_{P_k}^g = &\left[\frac{(-1)^{\frac{2}{\alpha}-1} \cdot (itP_T\psi w^\alpha)^{\frac{2}{\alpha}} \cdot \Gamma\left(-\frac{2}{\alpha}, -itP_T\psi w^\alpha (r+1)^{-\alpha}\right)}{-\alpha}\right]_0^R - \\ &- \left[\frac{(-1)^{\frac{1}{\alpha}-1} \cdot (itP_T\psi w^\alpha)^{\frac{1}{\alpha}} \cdot \Gamma\left(-\frac{1}{\alpha}, -itP_T\psi w^\alpha (r+1)^{-\alpha}\right)}{-\alpha}\right]_0^R.\end{aligned} \tag{4.33}$$

Lemma 2. *If $n \in \mathbb{N}$ and $z > 0 \in \mathbb{R}$ the incomplete Gamma function holds the following equality [19, pp. 177, eq. 8.4.13]:*

$$\Gamma(1-n, z) = z^{1-n} E_i(n, z),$$

where $E_i(n,z)$ is the exponential integral function, given by $\int_1^\infty \frac{e^{-zt}}{t^n}\ dt$ [78, pp. 490].

Applying Lemma 2 to (4.33), it can be simplified as:

$$\varphi_{P_k}^g = \left[\frac{(-1)^{\frac{-2}{\alpha}-1+\frac{2}{\alpha}}\cdot(r+1)^2\cdot E_i\left(1+\frac{2}{\alpha},-itP_T\psi w^\alpha(r+1)^{-\alpha}\right)}{-\alpha}\right]_0^R - \left[\frac{(-1)^{\frac{-1}{\alpha}-1+\frac{1}{\alpha}}\cdot(r+1)\cdot E_i\left(1+\frac{1}{\alpha},-itP_T\psi w^\alpha(r+1)^{-\alpha}\right)}{-\alpha}\right]_0^R, \quad (4.34)$$

and considering the upper and lower bounds of the integral, then

$$\varphi_{P_k}^g = \frac{1}{\alpha}\Bigg[(R+1)^2E_i\left(1+\frac{2}{\alpha},-itP_T\psi w^\alpha(R+1)^{-\alpha}\right) - E_i\left(1+\frac{2}{\alpha},-itP_T\psi w^\alpha\right) - \\ - (R+1)E_i\left(1+\frac{1}{\alpha},-itP_T\psi w^\alpha(R+1)^{-\alpha}\right) + E_i\left(1+\frac{1}{\alpha},-itP_T\psi w^\alpha\right)\Bigg]. \quad (4.35)$$

Accordingly, (4.31) can now be written as

$$\varphi_{P_k} = \frac{2}{\alpha\Gamma(k_\Psi)\theta_\Psi^{k_\Psi}R^2}\cdot\Bigg[\int_0^\infty e^{-\frac{\psi}{\theta_\Psi}}\cdot\psi^{k_\Psi-1}\cdot(R+1)^2E_i\left(1+\frac{2}{\alpha},-itP_T\psi w^\alpha(R+1)^{-\alpha}\right)\ d\psi - \\ - \int_0^\infty e^{-\frac{\psi}{\theta_\Psi}}\cdot\psi^{k_\Psi-1}\cdot E_i\left(1+\frac{2}{\alpha},-itP_T\psi w^\alpha\right)\ d\psi - \\ - \int_0^\infty e^{-\frac{\psi}{\theta_\Psi}}\cdot\psi^{k_\Psi-1}\cdot(R+1)E_i\left(1+\frac{1}{\alpha},-itP_T\psi w^\alpha(R+1)^{-\alpha}\right)\ d\psi + \\ + \int_0^\infty e^{-\frac{\psi}{\theta_\Psi}}\cdot\psi^{k_\Psi-1}\cdot E_i\left(1+\frac{1}{\alpha},-itP_T\psi w^\alpha\right)\ d\psi\Bigg]. \quad (4.36)$$

Lemma 3. *If $\mathbb{R}(n+\upsilon)>0$, $\mathbb{R}(\mu+\beta)>0$ and $|arg\beta|<\pi$ then [50, pp. 639, eq. 6.228.2]:*

$$\int_0^\infty E_i(n,\beta x)e^{-\mu x}x^{\upsilon-1}\ dx = \frac{\Gamma(\upsilon)}{(n+\upsilon-1)(\beta+\mu)^\upsilon}\cdot{}_2F_1\left(1,\upsilon;\upsilon+n;\frac{\mu}{\mu+\beta}\right),$$

where $E_i(n,z)$ is the Hypergeometric function as defined in [50, pp. 1005, eq. 9.100].

Since θ_Ψ, k_Ψ and $alpha \in \mathbb{R}_{>0}$, Lemma 3 can be applied to (4.36), such that

$$\begin{aligned}\varphi_{P_k} = &\frac{2}{\alpha\Gamma(k_\Psi)\theta_\Psi^{k_\Psi}R^2}\cdot\\ &\cdot\left[\frac{(R+1)^2\Gamma(k_\Psi)}{(k_\Psi+\frac{2}{\alpha})(\frac{1}{\theta_\Psi}-itP_Tw^\alpha(R+1)^{-\alpha})^{k_\Psi}}{}_2F_1\left(1,k_\Psi;k_\Psi+1+\frac{2}{\alpha};\frac{\theta_\Psi^{-1}}{\theta_\Psi^{-1}-itP_Tw^\alpha(R+1)^{-\alpha}}\right)-\right.\\ &-\frac{\Gamma(k_\Psi)}{(k_\Psi+\frac{2}{\alpha})(\frac{1}{\theta_\Psi}-itP_Tw^\alpha)^{k_\Psi}}{}_2F_1\left(1,k_\Psi;k_\Psi+1+\frac{2}{\alpha};\frac{\theta_\Psi^{-1}}{\theta_\Psi^{-1}-itP_Tw^\alpha}\right)-\\ &-\frac{(R+1)\Gamma(k_\Psi)}{(k_\Psi+\frac{1}{\alpha})(\frac{1}{\theta_\Psi}-itP_Tw^\alpha(R+1)^{-\alpha})^{k_\Psi}}{}_2F_1\left(1,k_\Psi;k_\Psi+1+\frac{1}{\alpha};\frac{\theta_\Psi^{-1}}{\theta_\Psi^{-1}-itP_Tw^\alpha(R+1)^{-\alpha}}\right)+\\ &\left.+\frac{\Gamma(k_\Psi)}{(k_\Psi+\frac{1}{\alpha})(\frac{1}{\theta_\Psi}-itP_Tw^\alpha)^{k_\Psi}}{}_2F_1\left(1,k_\Psi;k_\Psi+1+\frac{1}{\alpha};\frac{\theta_\Psi^{-1}}{\theta_\Psi^{-1}-itP_Tw^\alpha}\right)\right].\end{aligned} \tag{4.37}$$

Property 1. *Gauss hypergeometric function functional relationships [50, pp. 1008, eq. 9.131.1]:*

$$\begin{aligned}F(a,b;c;z) &= (1-z)^{-a}F\left(a,c-b;c;\frac{z}{z-1}\right)\\ &= (1-z)^{-b}F\left(b,c-a;c;\frac{z}{z-1}\right)\\ &= (1-z)^{c-a-b}F(c-a,c-b;c;z)\end{aligned}$$

Lastly, using the hypergeometric function property expressed in Property 1, (4.37) can be simplified as

$$\begin{aligned}\varphi_{P_k}(t) = \frac{2}{R^2(-itw^\alpha P_T\theta_\psi)^{k_\psi}}\cdot&\left[\frac{\mathbb{I}_1(1)-(1+R)^{1+\alpha k_\psi}\mathbb{I}_1((1+R)^\alpha)}{1+\alpha k_\psi}+\right.\\ &\left.+\frac{(1+R)^{2+\alpha k_\psi}\mathbb{I}_2((1+R)^\alpha)-\mathbb{I}_2(1)}{2+\alpha k_\psi}\right],\end{aligned} \tag{4.38}$$

where $\mathbb{I}_m(z) =_2 \mathrm{F}_1\left(k_\psi, k_\psi+\frac{m}{\alpha}, 1+k_\psi+\frac{m}{\alpha}, -\frac{iz}{tw^\alpha P_T\theta_\psi}\right)$. Since $\varphi_{P_j}(t) = \varphi_{P_k}(t)$, using (4.38) and (4.25), the probability of successful frame reception can now be rewritten as

$$\mathrm{P}[S|n_c] = 1-\frac{1}{2\pi}\int_{-\infty}^{0} e^{-ixt}\varphi_{P_j}\left(\frac{t}{b+1}\right)\cdot\varphi_{N_0}\left(-\frac{b}{b+1}t\right)\left(\varphi_{P_k}\left(-\frac{b}{b+1}t\right)\right)^{n_c-1}\mathrm{d}x, \tag{4.39}$$

which can be easily computed though the Fast Fourier Transform (FFT) algorithm.

4.2.4 Joint PHY/MAC Performance

In a n sized network as described in Subsection 4.2.2, the probability of a LoRa gateway successfully decoding a frame given n_c concurrent transmissions, such that $1 \leq n_c \leq n$,

can be computed using (4.39). However, when the medium access control layer is taken into account the number of devices involved in a collision (n_c) is not deterministic, but a time-varying random variable. As a result the probability of success must account not only for the likeliness of a frame being decoded given a collision involving n_c nodes, but also the probability of occurring such a collision. Thus, the probability of successfully decoding a frame when n nodes compete is given by

$$\mathrm{P}[S] = \frac{\sum_{k=1}^{n} k \ \mathrm{P}[S|k] \ \mathrm{P}[C=k]}{\sum_{k=1}^{n} k \ \mathrm{P}[C=k]}, \tag{4.40}$$

where $P[S|k]$ is the probability of success at the PHY layer given by (4.39) and $P[C=k]$ is the information from the MAC layer given by (4.10). Bearing in mind that the power received at the gateway from each LoRa ED is independent and identically distributed, coupled with that fact that it is assumed that multiple frames can be successful received simultaneously, the numerator of (4.40) can be seen as an approximation of the number of frames simultaneously received with success at the gateway, thus

$$\mathrm{E}[N_{rx}] \approx \sum_{k=1}^{n_c} k \ \mathrm{P}[S|k] \ \mathrm{P}[C=k]. \tag{4.41}$$

4.3 Performance Evaluation

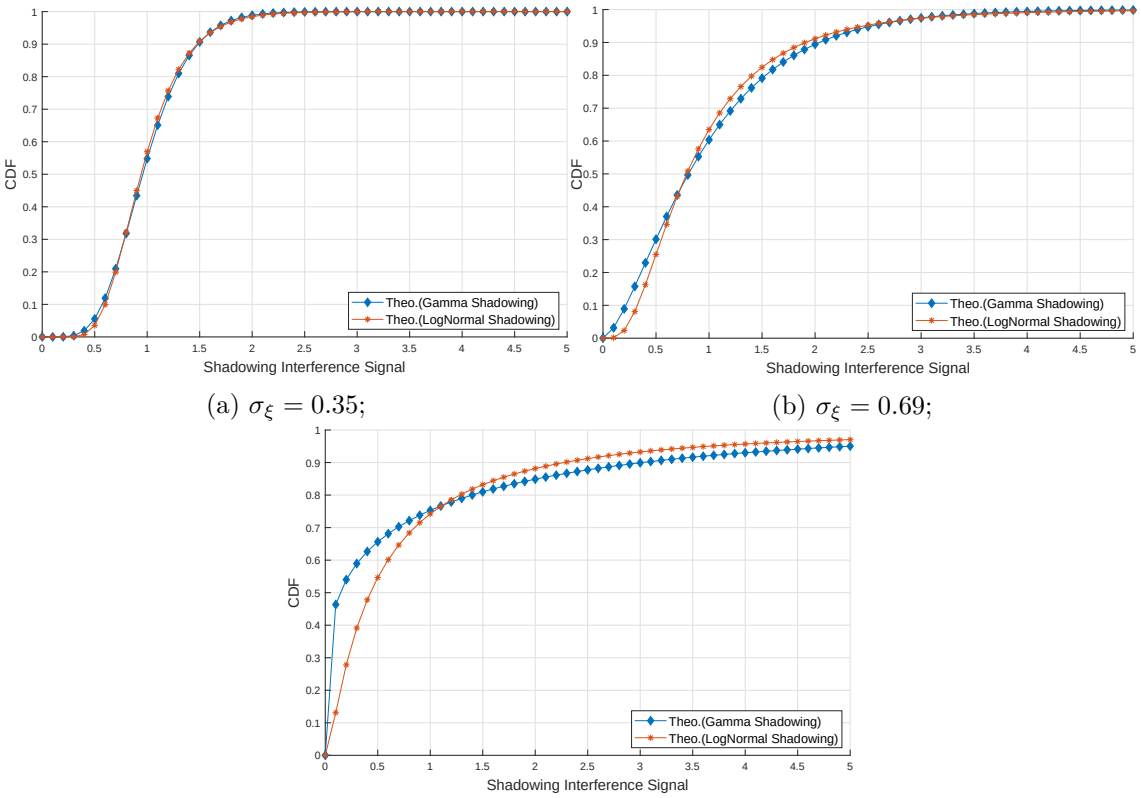
In this Section the accuracy of the performance model is assessed through the comparison of both numerical and simulated results. As mentioned in Section 4.2, this model analyses LoRa's uplink performance, as such, several different propagation conditions and traffic load scenarios were considered. This aims to reflect the impact that different propagation environments have on link outage.

Regarding the LoRa network scenario considered in the performance evaluation, and unless otherwise stated, it is considered to be a circular region with a radius $R = 1$ Km centered at the gateway. The network is operating at 868 MHz, occupying a bandwidth of 125 kHz. All devices adopt the same spreading factor (SF = 7) and transmission power ($P_T = 14$ dBm). The capture threshold was parameterized to $b = -6$ dBm [58], which allows the capture of multiple frames at the same time. Regarding the traffic model, we have considered each time unit equal to the frame's duration. The curves identified in the Figures as "Simu."and "Theo."correspond to values obtained through simulations and theoretical numerical calculations, respectively. Subsection 4.3.1 displays the validation of the model components. Shadowing log-normal and gamma distributions are compared to evaluate the approximation validity. The PDF values of the MAC layer Poisson distribution are compared to incidence rate of each concurrent transmission case obtained in the simulations. Finally the PHY success probability theoretical results were computed using the characteristic function of Υ (4.39) and contrasted with the probability

of success achieved in the simulations. Subsections 4.3.2 to 4.3.4 show the theoretical and simulated isolate and joint performance of each model layer.

4.3.1 Model Validation

In Subsection 4.2.2, the shadowing power was shown to be distributed according to a log-normal distribution (4.15). As aforementioned, this distribution proprieties make it mathematically intractable. For this reason, using the method described in [1], it was approximated to a gamma distribution (4.16). Figure 4.3 shows the validity of this approximation, especially for values of $\sigma_\xi < 1$ were the gamma and log-normal CDF curves are virtually overlaid. The values plotted in the graphics were calculated considering the respective distribution parameters as before established, i.e log-normal variance and mean as σ_ξ and $\mu_\xi = -\frac{\sigma_\xi^2}{2}$, respectively, and gamma shape and scale as $\vartheta = (e^{\sigma_\xi^2} - 1)^{-1}$ and $\omega_s = e^{\mu_\xi}\sqrt{\frac{\vartheta+1}{\vartheta}}$.



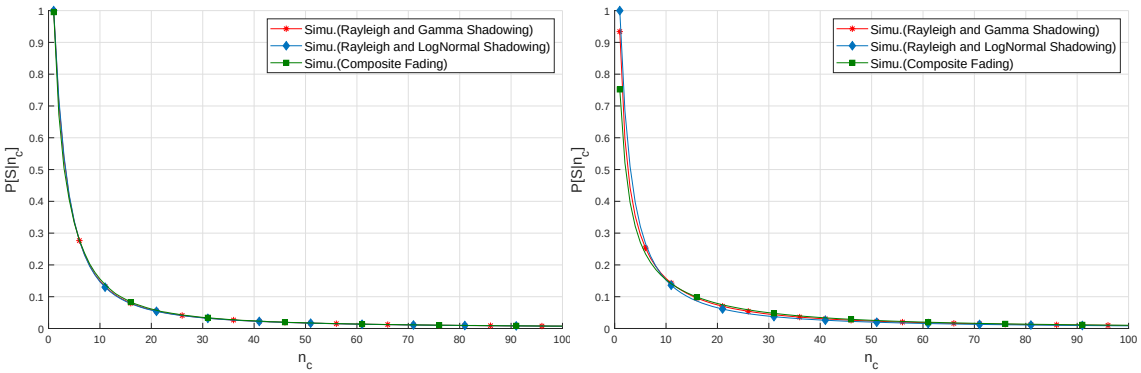
(a) $\sigma_\xi = 0.35$; (b) $\sigma_\xi = 0.69$;

(c) $\sigma_\xi = 1.3$;

Figure 4.3: Comparison of Shadowing LogNormal and Gamma approximation distributions CDF for different values of σ_ξ.

Accordingly, given the discrepancies between the gamma and log-normal CDF values for $\sigma_\xi > 1$, noticeable in Figure 4.3c, the PHY layer probability of success (4.39) was simulated considering three different small and large scale fading combinations. This was done as a means to evaluate the degree of disparity between the simulated curves, ascribable to the approximations. Three different composite fading combinations were compared. Rayleigh

fading (4.13) with normalized gain first combined with gamma shadowing and then log-normal shadowing. Lastly, the gamma joint fading (4.18), since it was approximated from a generalized k distribution using the method proposed in [3]. The composite fading gamma distribution parameterization is done though the shadowing gamma parametrization, i.e, its shape and scale are $k_\Psi = \frac{1}{\frac{2(\vartheta+1)}{\vartheta}-1}$ and $\theta_\Psi = (\frac{2(\vartheta+1)}{\vartheta} - 1)\omega_s$, respectively. As stated in the aforementioned Subsection, the generalized k is the distribution obtained from the combination of Rayleigh fading and gamma shadowing. The simulation results are displayed in Figure 4.4. Each n_c, i.e. each case from one to one hundred concurrent transmissions, was simulated one hundred thousand times to soothe curve distortion due to the random values generated in the simulation. Each simulated LoRa signal is affected by path loss and fading (4.21). The path loss exponent was considered to be $\alpha = 2.01$, while fading values were generated trough the respective Matlabs random generator functions, using the aforementioned distributions parameterizations. Additionally, Gaussian noise was considered at the gateway and generated though Matlabs exponential distribution random generator function with variance given by (4.19) with a noise figure of 6 dBs.



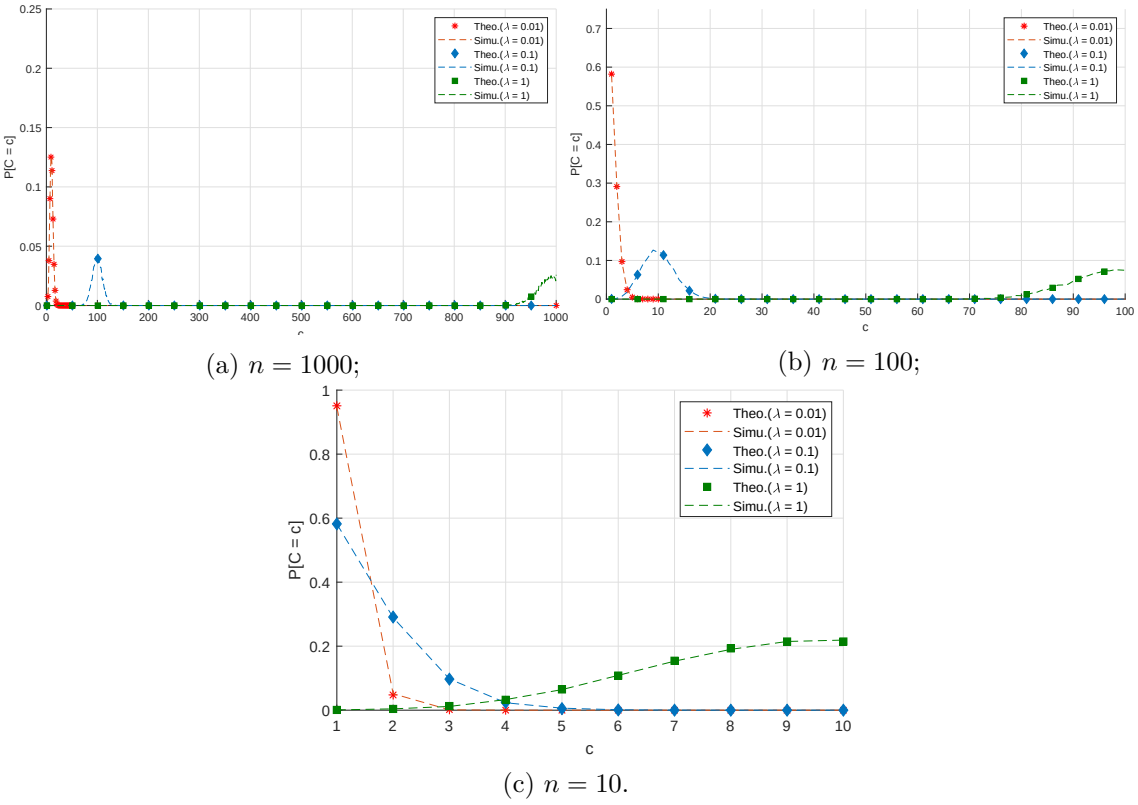
(a) $\sigma_\xi = 0.69$; (b) $\sigma_\xi = 1.3$;

Figure 4.4: Success probability of PHY layer given n_c concurrent transmissions considering different fading combinations.

Once again it is observable that for values of $\sigma_\xi < 1$ the curves are overlaid (Figure 4.4a), thus validating the gamma approximations. Conversely, when $\sigma_\xi > 1$ is considered, small disparities start to appear (Figure 4.4b). It is important to note that these differences are mostly noticeable in extremely low load scenarios, but become negligible otherwise.

The MAC layer validation was achieved by comparing the theoretical PDF values of the truncated Poisson distribution (4.10), which represent the access probability, with the rate of accesses obtained in the simulations. For that matter, a vector of n columns, being n the total number of nodes in the network, was created. Each column of the vector represents a case of concurrent transmissions, i.e the first column represents a single node transmitting, the second represents two concurrent transmissions and so on. Another vector of size s was created, being s the number of simulation repetitions. Through a matlab random generator function, which generates random values bases on an input distribution, the vector was populated with the number of concurrent transmissions per repetition of the simulation.

By iterating this vector, the first one was filled with the number of instances of each case, in the respective column. Finally, the simulated access probability was calculated by dividing the number of occurrences of each case by the number of simulations repetitions. Figure 4.5 shows the results obtained for different network sizes (n), considering $s = 10^4$ repetitions. It can be seen that the simulated probabilities match the theoretical values. Moreover, Figure 4.5 also depicts how the truncated Poisson distribution behaves depending on the network size and λ value used.



(a) $n = 1000$; (b) $n = 100$;

(c) $n = 10$.

Figure 4.5: Simulated and theoretical access probability for different network sizes and frames per time unit.

Regarding the PHY layer, the theoretical probability of success given n_c concurrent transmissions (4.39) was computed though the Fast Fourier Transform algorithm for several propagation conditions. Four scenarios were considered, namely, transmitted signals being affected solely by path loss with and without Gaussian noise at the gateway, then affected by path loss and composite fading, once again with and without Gaussian noise. In the scenarios without Gaussian noise its characteristic function (4.27) was considered to be unitary. The theoretical curves without composite fading were obtained by considering only the path loss characteristic (4.32) in the calculation of the received power characteristic function (4.30). The simulated results were obtained by forcing n_c sized collisions and registering the number of successfully received frames on a counter variable. Each n_c collision was repeated $s = 10^4$ times. The probability of success was then calculated through the ratio of successfully received frames over the total frames sent, which is given

by the number of concurrent transmissions times the simulation repetitions. This process was repeated for all four scenarios. For both the theoretical and simulated results, the path loss exponent was considered to be $\alpha = 2.01$ and the composite fading parameters were calculated according to $\sigma_\xi = 0.69$. The Gaussian noise was parameterized as previously mentioned. Lastly, the number of concurrent transmissions n_c was varied from one to ten. In Figure 4.6 it can be seen that the theoretical and simulated results are identical for all four propagation scenarios.

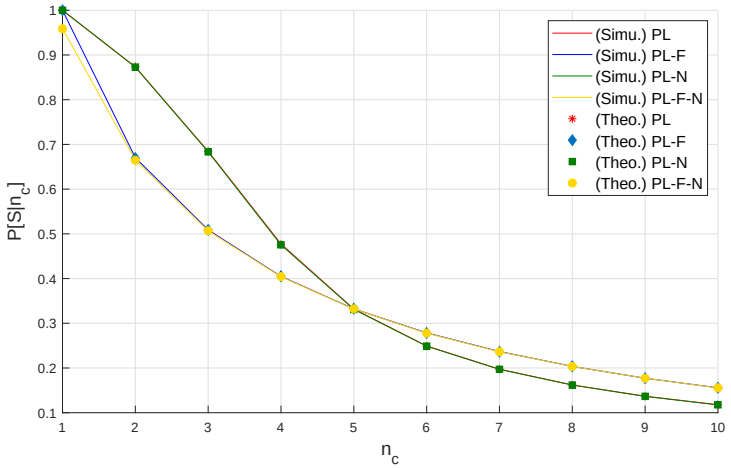


Figure 4.6: Theoretical and simulated probability of success given n_c concurrent transmissions.

4.3.2 MAC Layer

In order to characterized the MAC behavior given a n sized network in function of the load (G) two Figures were plotted. Numerical results for both Figures were computed with (4.10), which represents the probability of the number of competing nodes (c). The expected number of frames per time unit (λ) was varied from 0.01 to 1, meaning that the considered time between transmissions changed from one hundred to one time units. As stated in Subsection 4.3, it is considered that a time unit is equal to the duration of each frame. Accordingly, all nodes in the network adopt the same frame length. Figure 4.7 shows the load generated by $n = 10$ LoRa devices, according to the aforementioned λ values, therefore $0.1 \leq G \leq 10$ frames per time unit. Since the access probability is described as a Poisson process, the network load in this context represents the expected number of concurrent transmission. Thus, as can be observed in the figure, given a load of x, most likely there will be x concurrent transmissions. To better depict the MAC behavior these same results were plotted as surface in Figure 4.8a. Additionally, since LoRa networks generally feature an high node density, new values were computed for a network of $n = 1000$ and plotted in Figure 4.8c. Figures 4.8b and 4.8d represent the top down view of the respective surfaces and clearly illustrate the fact that the expected number of concurrent transmissions is equal to the load.

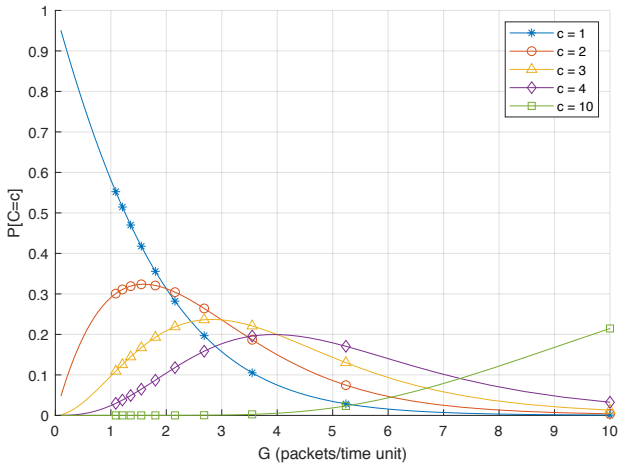
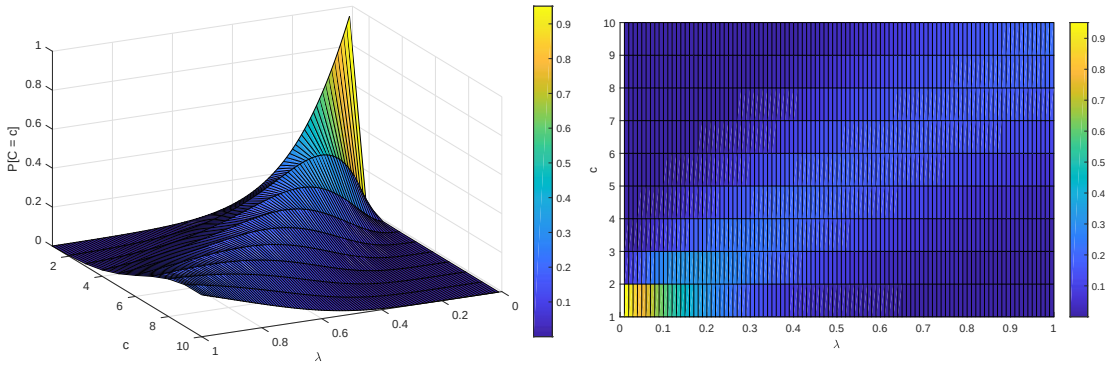


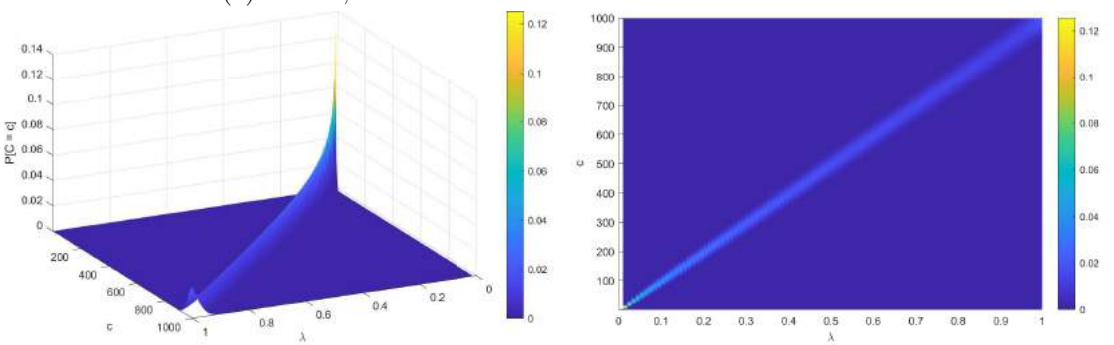
Figure 4.7: Probability of observing $c = 1, 2, 3, 4, 10$ concurrent transmissions.

Usually LoRa networks operate in the unsaturated traffic region, i.e., $G \leq 1$. For $G \leq 1$ we observe that the probability of having a single device accessing the medium ($c = 1$) is always greater than 0.5. As G increases from 0 to 1 the probability of only transmitting a single device decreases, but the probabilities of observing a collision between $c = \{2, 3, 4, 10\}$ devices increase. However, for $G \approx 1$ frames per time unit the probability of observing collisions involving 4 frames is close to zero, meaning that the occurrence of collisions involving 5 or more devices can be neglected for $G \leq 1$.



(a) $n = 10$;

(b) $n = 10$;



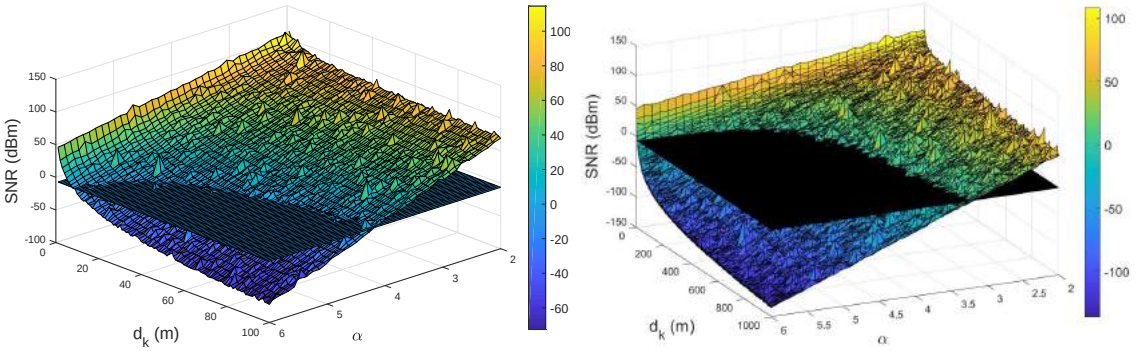
(c) $n = 1000$;

(d) $n = 1000$.

Figure 4.8: Probability of observing c concurrent transmissions.

4.3.3 PHY Layer

To portray the attenuation caused by path loss in a transmission, a scenario without fading, i.e. signals were only affected by path loss, was considered. In this simulation a single node transmits a frame. The node's Euclidean distance to the gateway (d_k) was varied from one to one thousand meters. For each node position the path loss exponent (α) was changed from two to six, to represent the different propagation environments showed in Table 4.1. To evaluate the contribution of path loss in link outage, per transmission the signal to noise ratio was calculated considering Gaussian noise at the gateway. The simulation was repeated 10^4 times per node position. Figure 4.9 displays the numeral results obtained as surface. The horizontal pane represents the SNR threshold value (b), given that $SF = 7$ was considered then $b = -6$ dBm. Signal to noise ratios above this plan represent successful frame receptions, otherwise there was link outage. To better contextualize the results, the Figure was divided into two scenarios. Figure 4.9a represents an indoor scenario, thus $1 \leq d_k \leq 100$ meters, while Figure 4.9b represents outdoor where $1 \leq d_k \leq 1000$.



(a) Indoor scenario;

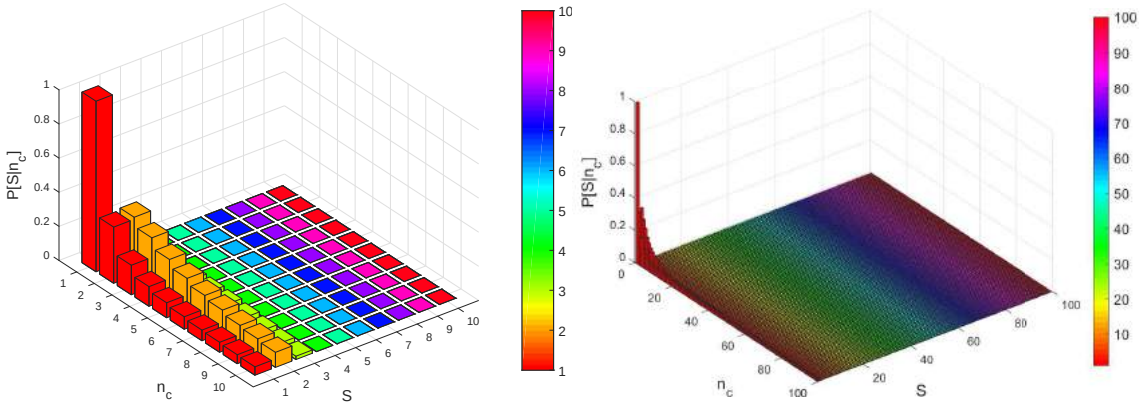
(b) Outdoor scenario;

Figure 4.9: Path loss effect on signal to noise ration.

In Table 4.1 indoor scenarios are divided into three distinct situations, in building with line of sight or obstructed, and in factory obstructed. By observing Figure 4.9a it can be concluded that in building obstructed transmissions are only viable up to approximately 35 meters, while with line of sight and in a obstructed factory settings the signal can be received with no problems. Regarding the outdoor scenario, there are two situations, urban and shadowed urban. Figure 4.9b shows that the achievable range varies greatly. In ultra high density urban settings link outage might start to happen as close as up to 100 meters, conversely in low building density environments, the gateway can easily decode frames sent from EDs located a thousand meters away. It is important to note that these results are only meant to characterize the effect of path loss in a single link scenario, thus are not representative of a real world situation were interference and fading have to be taken into account.

The probability of successfully decoding a frame given n_c concurrent transmissions

(4.25) constitutes the sum of the individual probability of success of x nodes, where $0 \leq x \leq n_c$. This means that the probability of success given four concurrent transmissions will be the probability of one frame being received plus the probability of two frames being received and so on. Similarly to the method described in Subsection 4.3.1, to compute these results, collisions of size n_c were forced, where $1 \leq n_c \leq n$, being n the total number of nodes in the network. For each value of n_c, the number of x successes was stored in a variable, e.g. for $n_c = 2$ it was stored the number of times one and two frames were successfully received. Each n_c was simulated 10^4 times. Figures 4.10a and 4.10b show the obtained numerical results for a network of ten and one thousand nodes, respectively.



(a) $n = 10$; (b) $n = 1000$;

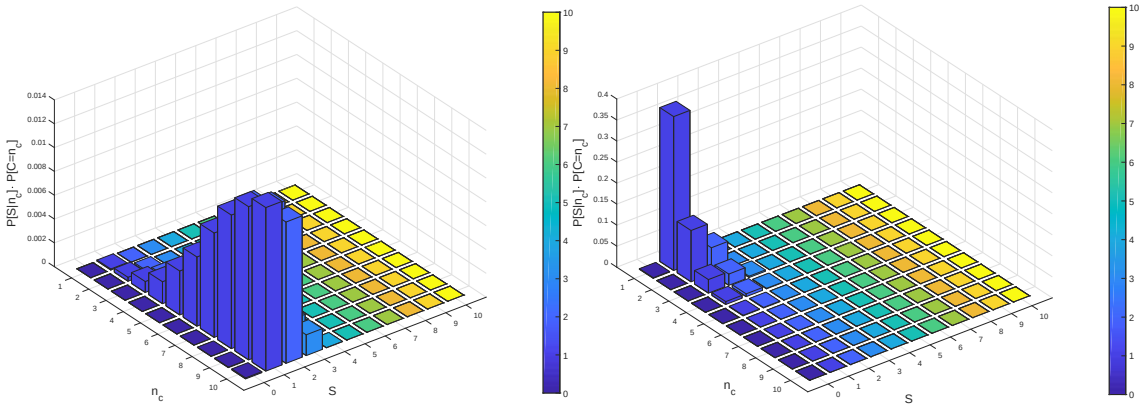
Figure 4.10: Individual success probability in different sized networks.

In the former, by comparison with Figure 4.6 it can be seen that the sum of the individual success probabilities will indeed amount to the success probability of a transmission given n_c collisions. Figure 4.10b shows that for collisions of over 20 frames the probability of success is approximately zero.

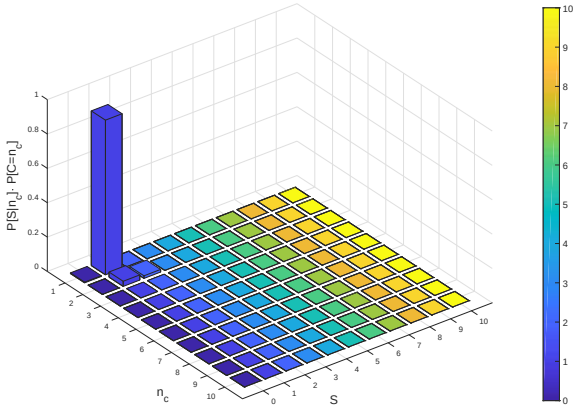
4.3.4 Joint MAC-PHY Model

Figure shows the influence of the MAC layer in success probability (4.40) of a network composed by 10 nodes. The results were simulated akin to the previously mentioned method used to compute the results plotted in Figure 4.10. However, instead of forcing collisions, they were generated through the Poisson distribution denoting the access probability (4.10). Consequentially, the number of collisions will be thoroughly dependent on the network load G. In the figure it is possible to verify that most prevalent collision size (n_c) coincides with the access probability expected value, which is equal to $n\lambda$, i.e. the network load. Naturally, as predictable, it can also be seen how the success probability decreases as the expected collision size increases. Figure 4.11a depicts a dramatic performance decrease caused by the network operating at maximum interference levels, i.e. the expected number of concurrent transmissions being equal to the total number of nodes in the network. Figures 4.11b and 4.11c show similar results, despite the latter having a load ten times

bigger. This is attributed to the fact that the expected value changed from 0.1 frames to one frame per time unit, meaning that transmissions wont be affected by interference the majority of the time. As a result link outage will be mostly caused by path loss and fading, given that the network spans over an area of only one kilometer, very few frames will arrive at the gateway with a SNR bellow the threshold value $b = -6$ dBm.



(a) $\lambda = 1$; (b) $\lambda = 0.1$;

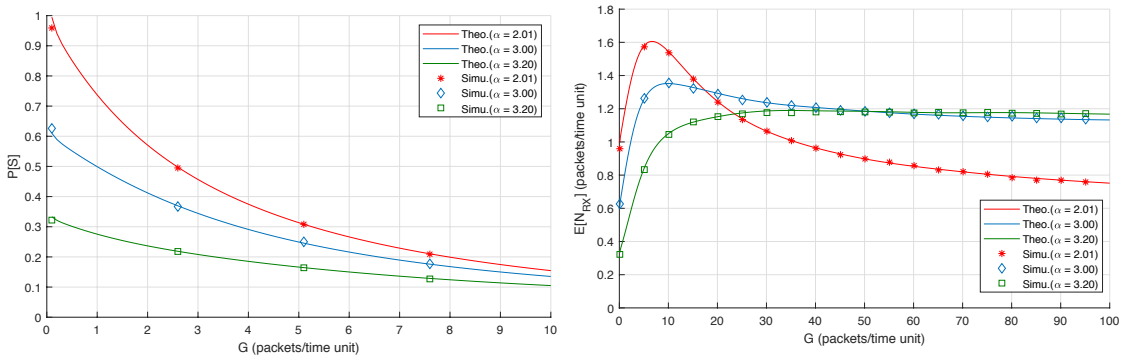


(c) $\lambda = 0.01$.

Figure 4.11: Success probability given n_c collisions as a function of the access probability.

In Figure 4.12 numerical and simulated results are compared. The results were obtained for the same scenario, where the number of devices, n, was changed from 1 to 1000 nodes and was considered that each device generates an average of $\lambda = 0.1$ frames/time unit. The multiple curves represent the performance for different path loss coefficients, α, and composite fading was parameterized with $\sigma_\xi = 0.69$. The numerical results are represented by the solid lines, while the simulation results are represented by the markers. The simulation results represent the average of 10^5 simulations. Figure 4.12a plots the probability of receiving an individual frame at the gateway, $\mathrm{P}[S]$, and the numerical results were computed using (4.40). Figure 4.12b plots the expected number of successful frames received at the gateway, $\mathrm{E}[N_{rx}]$, and the numerical results were computed with (4.41). For both $\mathrm{P}[S]$ and $\mathrm{E}[N_{rx}]$ it can be observed that the numerical results are close to the simulation results, showing the accuracy of the performance model proposed in this chapter.

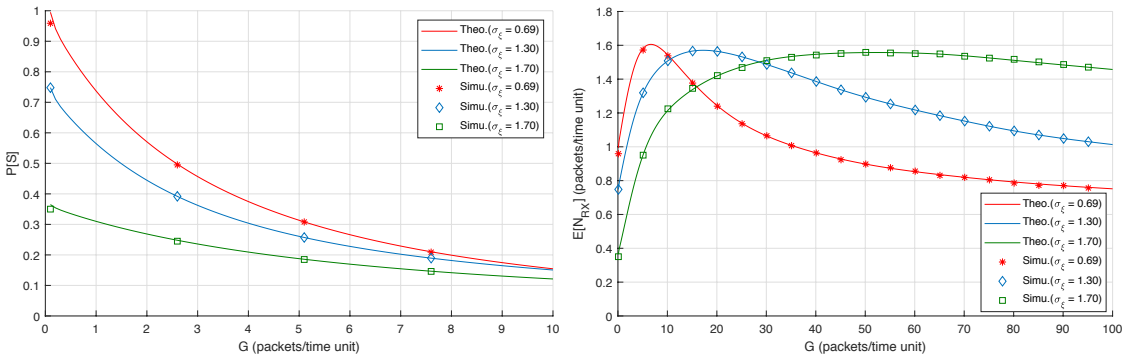
P[S] decreases as the network load increase and lower P[S] values are observed for higher path loss coefficients. E[N_{rx}] achieves a maximum that depends on the path loss coefficient. As depicted in Figure 4.12b, more frames can be successfully received for lower path loss coefficients.



(a) (b)

Figure 4.12: (a) Successful frame reception probability (P[S]) for different path loss scenarios, α; (b) Average number of successful received frames (E[N_{rx}]) for different path loss scenarios, α.

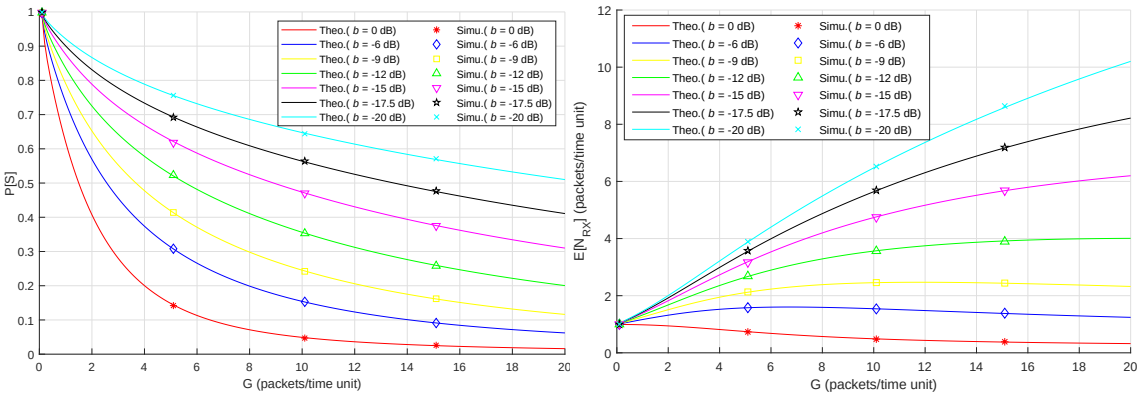
Figure 4.13 also depicts the characterization of P[S] and E[N_{rx}]. However, the results were obtained for a constant path loss coefficient ($\alpha = 2.01$) as a means to assess the impact of fading in the success probability. This was done by considering different fading uncertainties, being that the fading uncertainty increases with σ_ξ. As can be seen in Figure 4.13a, the probability of successfully receiving a frame decreases as the fading uncertainty increases. Regarding E[N_{rx}], it can be observed in Figure 4.13b that higher fading uncertainty move the optimal point of operation to the right, meaning that the increase of fading uncertainty can only be compensated through the increase of the network's traffic load. Once again, the simulation results are close to the numerical results, confirming the accuracy of the proposed model.



(a) (b)

Figure 4.13: (a) Successful frame reception probability (P[S]) for different shadowing scenarios, σ_ξ; (b) Average number of successful received frames (E[N_{rx}]) for different shadowing scenarios, σ_ξ.

In Figure 4.14 the impact of the different spreading factors was studied considering the same scenario of Figure 4.12, i.e. the path loss exponent and composite fading parameters were assumed to be $\alpha = 2.01$ and $\sigma_\xi = 0.69$. The curves in the figure represent the cases when the spreading factor 7, 8, 9, 10, 11, and 12 are adopted by the nodes and the gateway, which correspond to $b = \{-6, -9, -12, -15, -17.5, 20\}$ dB [58], respectively. As the spreading factor increases, b decreases and, consequently, the average number of successfully received frames increases. The curves confirm that higher spreading factors allow more frames to be successfully decoded at the same time. The average number of frames successfully received also vary with the network's load, and has a maximum for all considered spreading factors. Finally, a curve for $b = 0$ dB was included in the plotted results. It is important to note that although $b = 0$ dB does not represent any spreading factor adopted by LoRa, it was included for comparison purposes, because it represents the case when only a single frame is captured at a given time instant. By comparing the curve for b =0 dB with the other curves, it is possible to highlight the gain of adopting a multi-capture receiver when compared to the case when at most a single frame is received.



(a) (b)

Figure 4.14: (a) Successful frame reception probability (P[S]) for different path loss scenarios, α; (b) Average number of received frames (E[N_{rx}]) for different values of b (for $\alpha = 2.01$ and $\sigma_\xi = 0.69$).

CHAPTER 5

Measured LoRa Performance

In contrast to the theoretical approach described in the last chapter, this chapter focuses on the performance of available hardware. As such, a basic network, composed by a gateway, and a single LoRa end device (ED) was deployed. The purpose of these tests was to collect empirical data with the intent of characterizing the viability of a LoRa network in different environments. As previously mentioned LoRa networks, both by design as well as regulatory impositions (Chapter 3), operate in the unsaturated traffic region. Thus, despite the limited hardware available for testing, the data collected can still be used as a reference point of what can be expected, performance wise, in a moderately sized LoRa network deployed in a setting with similar conditions.

All of the hardware used was provided in a LoRa/LoRaWAN kit, assembled by Seed Studio, which contains all the basic elements necessary to perform these measurements.

5.1 LoRa Node

The node, a Seeeduino LoRaWAN with GPS, is an Arduino compatible development board with LoRaWAN protocol and GPS embedded. The LoRaWAN module is based on the communication module RHF76-052AM [54]. It is a single channel LoRa radio, meaning it can only receive or send a frame at a time [49]. The channel can be configured for any sub band in the 868 MHz frequency band, where LoRa operates, and receive/transmit frames, in the set frequency channel, using any available data rate. Using LoRa's adaptative data rate mode, the board can transmit on any channel available using any data, provided that these channels are listed in a pre-configuration [49]. In the same way as Arduino, the board can be programmed via a micro-USB connection, using the Arduino IDE. Additionally, it can be powered directly through the micro usb port or alternatively using a 3.7 V Lipo battery. As such, it comes equipped with an integrated lithium battery management chip,

which can be used for charging as well as providing battery power measurements [54].

As can be seen in Figure 5.1, the node was equipped with some rudimentary components. Two modes of operations were implemented. The first is a manual mode, in which a single packet using spreading factor 7 with a bandwidth of 125 kHz, is sent by pressing button two. In manual mode packets can be transmitted in four different ways:

- **Single channel without confirmation** - A frame is sent in the 868.1 MHz frequency channel, without requesting confirmation of reception;
- **Single channel with confirmation** - A frame is once again sent in the 868.1 MHz frequency channel, but now requests the gateway to send a reception acknowledgment;
- **Multi channel without confirmation** - A frame is sent on one of the pre-configured channels, without acknowledge;
- **Multi channel without confirmation** - A frame is sent on one of the pre-configured channels, requiring acknowledge;

These can be selected by simultaneously pressing the two buttons. It is important to point that this mode was only implemented to facilitate debugging and provide an easy method to verify if the network is operational and functioning as supposed. As such, none of the results exhibited in this chapter were obtained in this way.

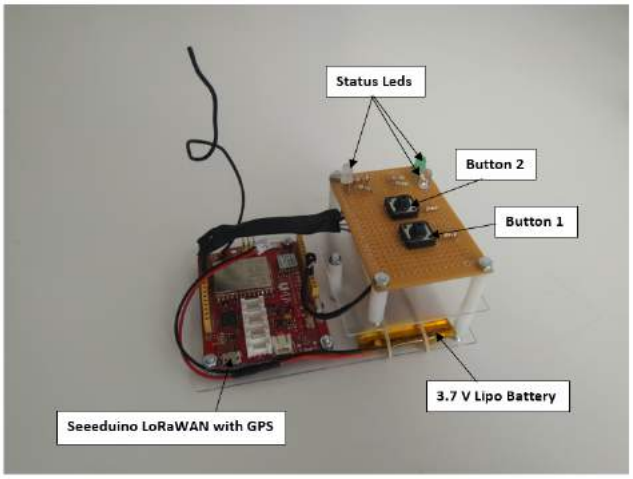


Figure 5.1: Assembled node.

The second mode, automatic mode, which is activated by pressing button one, automatically sends n packets per spreading factor, which means a total of $6 \times n$ packets per test. All frames are sent in the 868.1 MHz frequency channel with a bandwidth of 125 kHz. These frames are sent every 5 seconds, thus being that 50 frames were sent per SF, each test has a duration of 25 minutes. In both modes the node is configured with ADR and duty cycle limitation turned off. Additionally, the node is initiated in ABP mode. Thus, as mentioned in Subsection 3.3.2.1, the application key as well as the application and network session key where directly coded into the developed script.

5.2 LoRa Gateway

As can be seen in Figure 5.2, the gateway is composed of three main components. A Raspberry Pi 3, a gateway module, and a bridge adapter. The former, a single board computer, is responsible for processing all the data received from the gateway module. It was loaded with an SD card, provided in the kit, containing a Raspbian image already loaded with the software necessary to integrate the gateway module, as well as a local server where the received data can be monitored. The RHF0M301-868 gateway module is based on Semtech's SX1301 digital baseband ship [13], which is a smart baseband processor specifically designed to offer high performance capabilities for long range ISM communication (15 Km with line of sight and 3 to 5 Km in urban environments) [59]. It features ten channels with differentiated levels of programmability. The first eight channels, IF0 to IF7, are limited to a bandwidth of 125 kHz, but can be individually configured to receive/transmit in different sub band segments (Section 3.4). Each channel can receive any data rate, without needing configuration. Furthermore, several packets received in the same channel can be decoded, provided that they were sent different data rates. The ninth, IF8, can be configured for every LoRa data rate and bandwidth, i.e. 125, 250 and 500 kHz, however, conversely to IF0-7 it can only decode frames sent using a data rate previously configured. The last channel, IF9, features the same configurations proprieties of IF8, but is meant for GFSK signals [59]. Sensitivity levels for SF7 to SF12, vary from -125 to -139 dBm [13], respectively. The last component, PRI 2 Bridge RHF4TOO2, is an adapter that enables the raspberry pi and the gateway to be directly connected. Lastly, a short monopole antenna, more specifically a 0 dBi rubber duck antenna, is used.

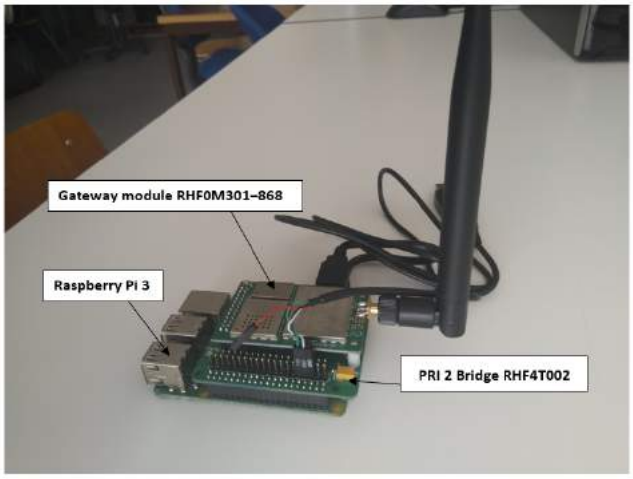


Figure 5.2: Lora gateway.

As mentioned in Subsection 5.1, the node is setup in Activation by Personalization mode. As such, the respective keys required for the node to be accepted into the network were registered in the gateway though its local server GUI. During all the performed test, the gateway was located in building (Figure 5.3). In Figure 5.3b it can be seen that

building is an prime example of tough propagation environment, since it has metal blinds and quite thick concrete walls (approximately 30 cm). Granted, this positioning is an hindering factor in the overall network performance. As a result the aforementioned 3 to 5 km of range are not to be expected, especially for EDs positioned in a way that the signals arrive through the opposite side of the building.

(a) Inside view; (b) Outside view;

Figure 5.3: Gateway location.

5.3 Test Sites

In a wireless network, the positioning of antennas is of utmost importance. For optimal performance, the majority of electromagnetic wave propagation should follow an unobstructed path between the transmitting and receiving antennas. In short communication links, line of sight is easy to achieve. However, as the distance between antennas starts to grow past a few kilometers, earth's curvature has to be taken in account. Against this background, data was collected from 9 locations in total. These were chosen such that the transmission link experienced different propagation conditions.

Test Site	**Latitude (degrees)**	**Longitude (degrees)**	**Distance (m)**
1	38.66140	-9.20534	125
2	38.66232	-9.20597	240
3	38.66264	-9.20593	275
4	38.66375	-9.20645	405
5	38.66469	-9.20012	645
6	38.66480	-9.21761	1210
7	38.64346	-9.22300	2442
8	38.64413	-9.23963	3507
9	38.72740	-9.22706	7203

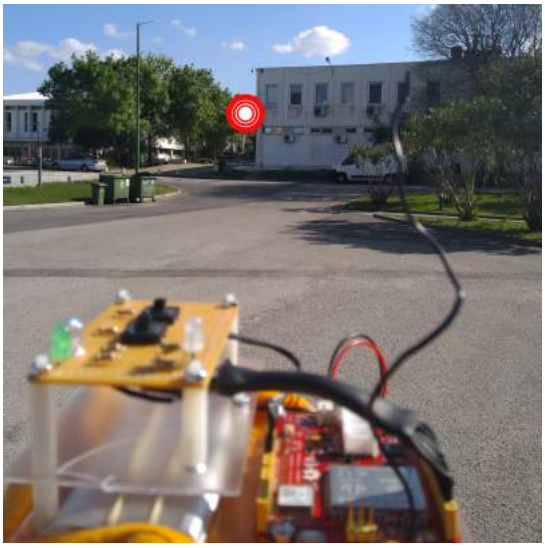
Table 5.1: Test site geographic locations and approximate distance to the gateway.

As can be seen in Table 5.1 the node was positioned as close as 125 meters up to 7 kilometers. Figure 5.4 shows the order in which the test were performed as well as the gateway position (red and white dot) relative to the test sites.

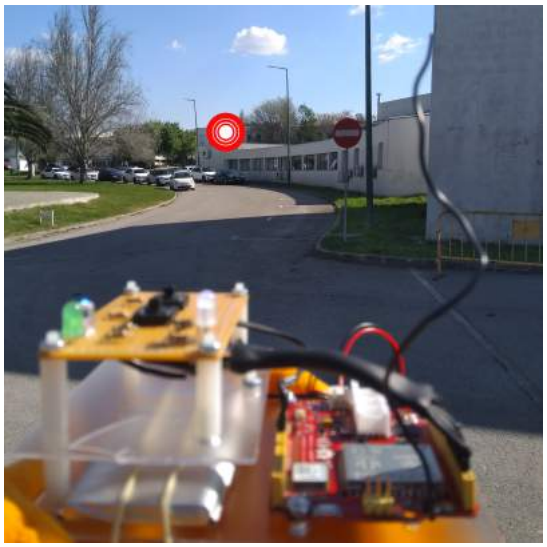
Figure 5.4: Test sites locations.

The first three sites are located inside the university campus, however none has direct line of sight. The first is located behind the physics department, the other two are in the vicinity of the university library. In all of these the node was placed at about one and half meters above ground level, facing the window where the gateway is positioned (which is on the right side of the building). The fourth site, as seen in Figure 5.4, is in direct alignment with the previous, but due to being a slightly higher local it holds line of sight. In the fifth one, the building, were the gateway is positioned, is in direct line of sight, however the signal still has to traverse the building wall to reach it. The sixth location is aligned with the gateway window without line of sight. However, conversely to the first three sites the signal path is mainly blocked by small elevations in an open field. The seventh and eighth locations are both facing the back side of the building. The former is located in an high lookout point, however the signal path is block by an hill with dense vegetation. The later is next to the coast, in a low density urban environment. In addition to building, the signal still as to traverse though hills and vegetation, as well as an highway with moderate traffic. The last test site is located at the highest point and features direct line of site. Figure 5.5, puts into perspective the previous descriptions, as it shows a picture of all the locales as well as their respective elevation relative to the sea level. The red and white circle seen in each picture is the marker that denotes the path a signal has to traverse to reach the gateway.

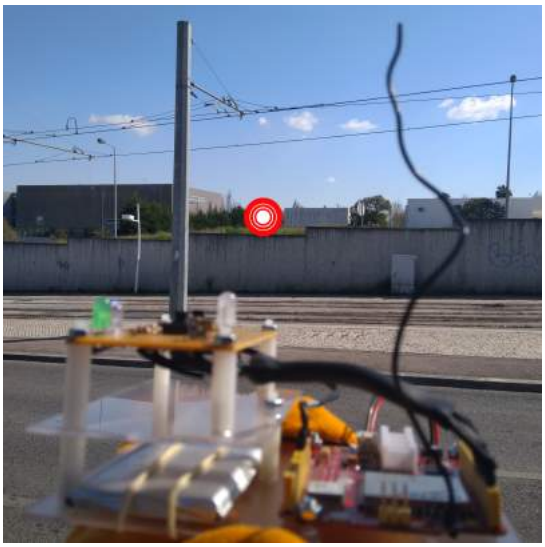
(a) Test site 1 (95 meters);



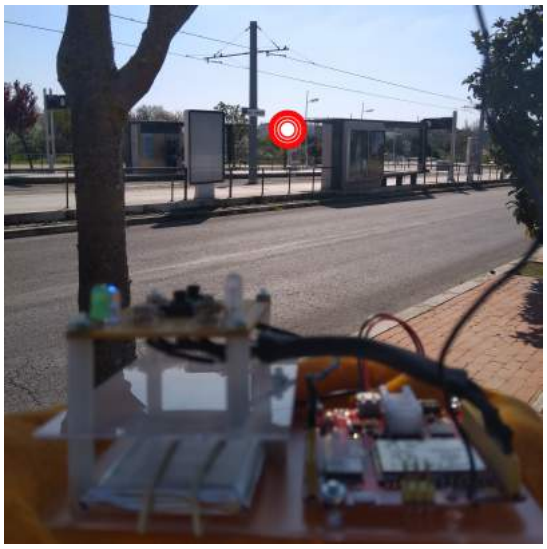
(b) Test site 2 (92 meters);



(c) Test site 3 (92 meters);

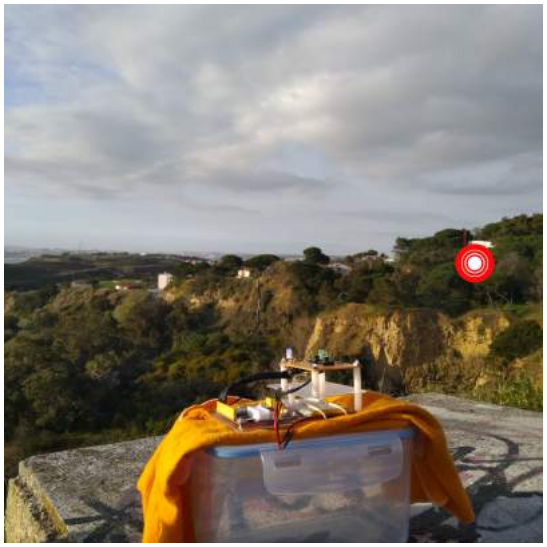


(d) Test site 4 (93 meters);



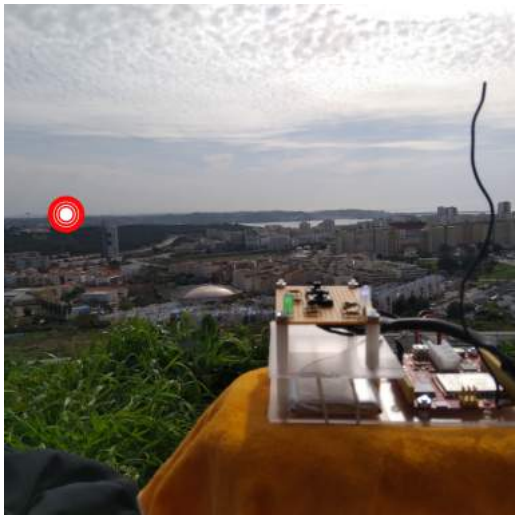
(e) Test site 5 (105 meters);

(f) Test site 6 (104 meters);



(a) Test site 7 (94 meters);

(b) Test site 8 (5 meters);



(c) Test site 9 (126 meters);

Figure 5.5: Gateway position relative to each test site, and the respective test sites elevation above see level.

5.4 Performance evaluation

Wireless environments can be highly unpredictable, in addition to physical phenomenons mentioned in Subsection 2.5.1, climate conditions can also hinder RF wave transmissions. High speed winds can misalign antennas or abnormal levels of air moisture can add attenuation to the signal path. For all these reasons the collected data is only representative of what to expect performance wise in a LoRa link deployed in similar conditions to the ones described in the previous section.

Table 5.2 lists the packet error rate (PER) per spreading factor of each test site. These values represent the complement of the probability of success plotted in Figure 5.6. The probability of success was calculated trough the ratio of received frames over the total

frames sent per spreading factor.

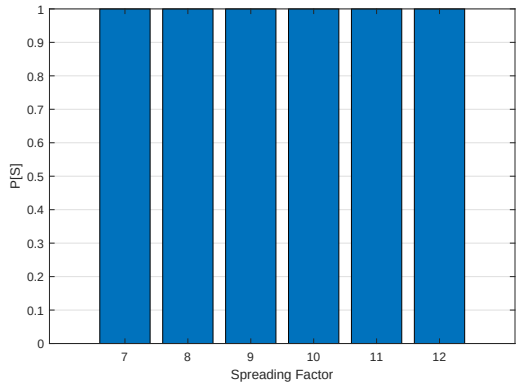
Test Site	PER(%)					
	SF7	**SF8**	**SF9**	**SF10**	**SF11**	**SF12**
1	0	0	0	0	0	0
2	4	0	0	0	0	0
3	100	88	34	30	2	2
4	0	0	0	0	0	0
5	98	76	64	42	16	18
6	100	100	100	96	98	94
7	100	100	100	100	100	100
8	100	100	100	100	100	100
9	100	100	82	2	0	0

Table 5.2: Packet Error Rate (PER) for each spreading factor per test site.

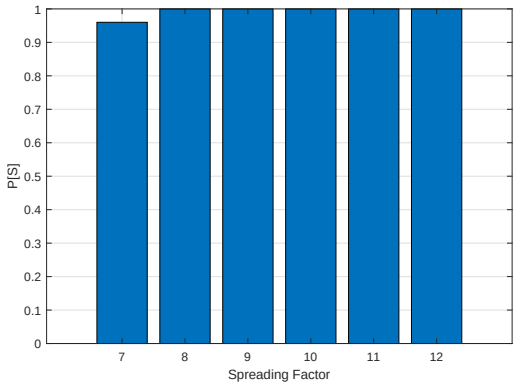
Examining the results in the aforementioned Table jointly with the plotted graphs it can be concluded that the best performance was achieved in test sites 1 and 4. This is not surprising, given that these are the locations closest to the gateway, without and with line of sight respectively. The frames sent from test site 2 were almost received in the totality, which is to be expected, since the propagations conditions are identical to the first test site. Test site 3, despite being only a few meters apart from test sites 1 and 2, displays steep decrease in overall performance. None of the spreading factor could be received in their totality. This detriment in link performance is most likely a direct consequence of the extra building blocking the signal path to the gateway. Frames sent from test site 5, despite having direct line of sight with the gateway building, display a PER of over 50 percent for spreading factors 7 to 9. However, the majority of frames sent with spreading factors 11 and 12 were successfully received. This means that lower SF signals do not have enough resilience to be able to penetrate the thick walls blocking the path to the gateway. By far, the worst performances come from test sites 6, 7 and 8. The results obtained from test sites 7 and 8 were expected. These locations feature the most adverse propagations conditions of all the test sites. In test site 8, despite being sent from an elevated position, signals had to traverse trough a hill sporting trees with quite dense foliage, tantamount, signals from 9 were obstructed not only by high buildings (with an average of five floors), but also by an highway surrounded by small hills and the occasional trees. In addition to all this, both positions are in alignment with the back side of the gateway building, i.e. provided that a signal manages to reach it, it still has to travel trough several concrete walls to reach the gateway. The results from test site 6 were expected to be akin to 3, with a slight decrease in performance. In this position the signal path is blocked by two buildings, aligned with the gateway window, as well as small hills in an open field. It is not possible to pin point the exact cause of this poor performance, but most likely it was caused by an unknown obstacle in the signal path. Lastly, results from test site 9 were surprising, since it was expected that only signals sent with SF 12 and maybe some with SF

11 would be received. However, close to hundred percent of the frames sent with SF above 10 were received, and even a small percentage of the ones sent with SF 9. These results prove LoRa's long range capabilities provided a link with line of sight. Furthermore, this performance is in conformity with the range reported in Section 5.2. Overall it can be said that the measured results fall in line with the expected outcomes and can be considered quite positive given the gateway positioning.

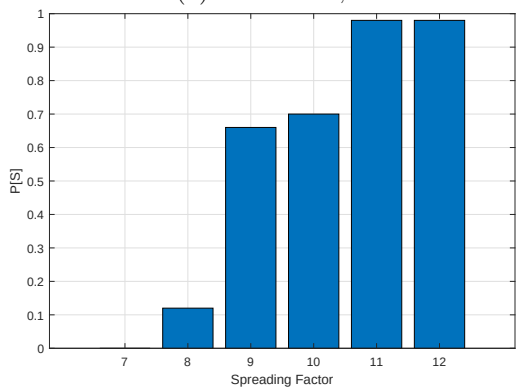
Tables 5.3 and 5.4, respectively, show the average signal to noise ratio and received signal strength indicator (RSSI) values obtained in the tests. These represent the ratio between the sum of all SNR or RSSI values retrieved from the gateway, over the total number of frames received per spreading factor. RSSI values represent a baseline for the expected power levels of signal derived from each test site.



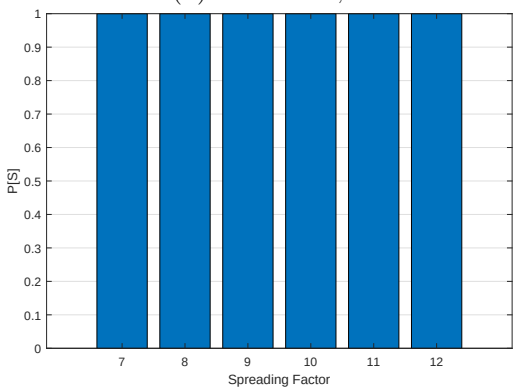
(a) Test site 1;



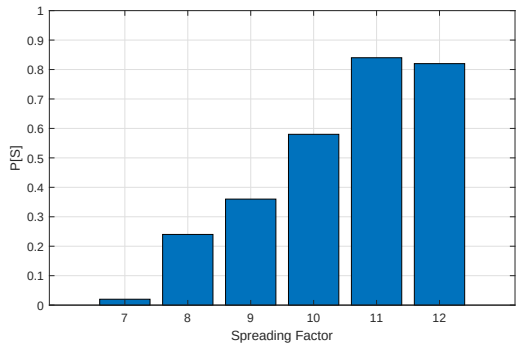
(b) Test site 2;



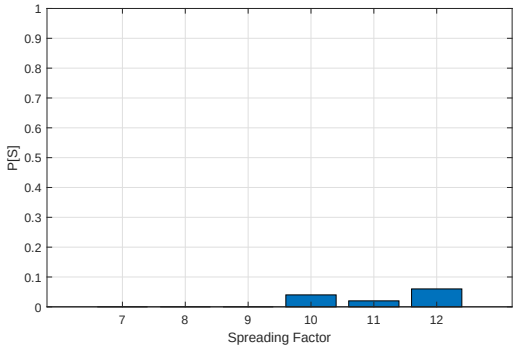
(c) Test site 3;



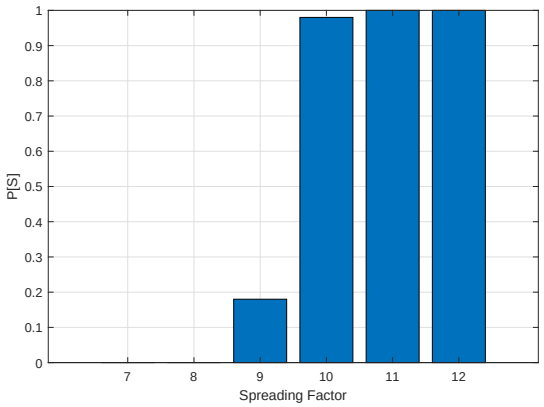
(d) Test site 4;



(e) Test site 5;



(f) Test site 6;



(a) Test site 9;

Figure 5.6: Success probability for each test site.

Test Site	Average SNR (dB)					
	SF7	**SF8**	**SF9**	**SF10**	**SF11**	**SF12**
1	5.6370	5.4250	5.2120	4.6860	4.2470	3.7570
2	-4.7333	-4.8940	-5.6920	-5.0200	-4.5160	-4.9360
3	-	-10.7000	-10.4576	-13.5686	-10.2980	-12.1878
4	1.7040	3.0700	4.1000	3.8800	3.9240	3.6180
5	-9.0000	-8.6083	-10.8611	-10.6414	-10.6452	-10.4098
6	-	-	-	-15.1000	-16.2000	-18.4333
7	-	-	-	-	-	-
8	-	-	-	-	-	-
9	-	-	-13.7222	-13.6918	-13.3480	-12.7740

Table 5.3: Average Signal to noise ratio for each spreading factor per test site.

Test Site	Average RSSI (dBm)					
	SF7	**SF8**	**SF9**	**SF10**	**SF11**	**SF12**
1	-101.0000	-102.3500	-104.2300	-102.2100	-103.3100	-100.8000
2	-108.2292	-109.1600	-109.8200	-108.8800	-108.5600	-108.3600
3	-	-110.3333	-110.8485	-110.6000	-110.8776	-110.6735
4	-105.0200	-104.4200	-104.6800	-102.5200	-103.5400	-104.2000
5	-108.0000	-109.0000	-108.9444	-109.2414	-109.0714	-109.2927
6	-	-	-	-108.0000	-109.0000	-108.0000
7	-	-	-	-	-	-
8	-	-	-	-	-	-
9	-	-	-108.4444	-108.4490	-108.3400	-108.2600

Table 5.4: Average RSSI for each spreading factor per test site.

These results were extracted directly from the RHF0M301-868 gateway module local server, as such, a small margin error is to be expected. This discrepancies are derived from the hardware specific method used to calculate RSSI values, which is dependent of the SNR value [13].

Figure 5.7 plots the density of packets received relative to SNR and RSSI values. These were obtained by aggregating all the SNR and RSSI values collected amongst all the performed tests. As aforementioned values of SNR lesser than zero decibels, represent signals received under the noise floor. In Figure 5.7b it can be seen that the gateway was able to decode frames that arrived with power up to ten times lower than the noise (-20 dB). Additionally, it can be verified that the majority of signals received bellow the noise floor are much weaker, reaching the point were it would be expected that they would drown in noise and be lost. Figure 5.7d shows that approximately the same density of packets were received above and under the noise floor. Once again it can be said that the results were satisfactory. As it could be checked, LoRa modulation is easily capable of decoding really weak frames whose signals to noise ratios indicate that they are well bellow the noise floor.

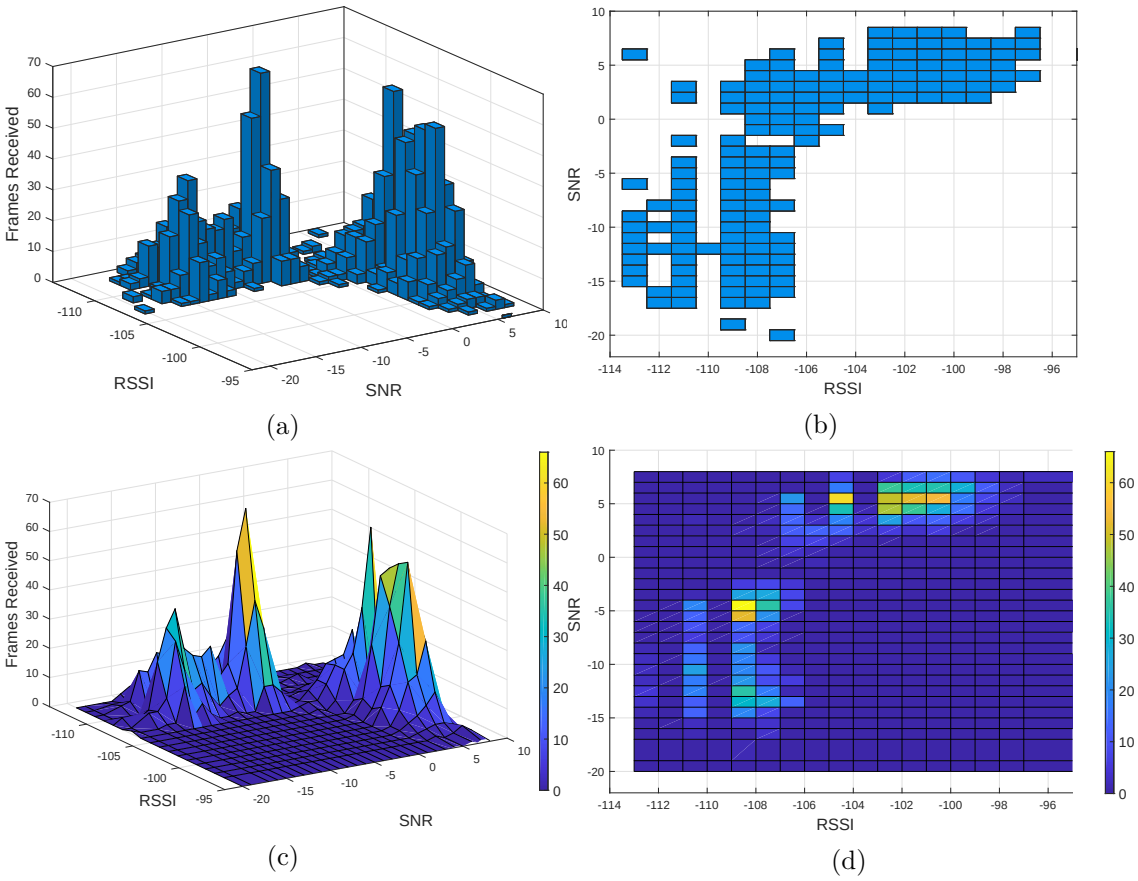


Figure 5.7: Characterization of the SNR and RSSI values received at LoRa's gateway.

CHAPTER 6

Conclusions

6.1 Final Remarks

This thesis explores LoRa's suitability and performance within the IoT paradigm. A LoRa's performance model is proposed, which adopts a typical LoRaWAN operating scenario, where the transmissions of LoRa Class A devices are affected by path-loss, shadowing and Rayleigh fading. A gamma distribution is adopted to represent the composite effects of shadowing and Rayleigh fading. Due to the possibility of capturing multiple frames simultaneously, theoretical and simulated results compare the maximum achievable performance of the PHY/MAC LoRa scheme according to the Signal-to-interference-plus-noise ratio capture metric. The contribution of this work is primarily focused on studying the average number of successfully received LoRa frames, which constitutes a performance upper bound due to the optimal capture condition considered in the PHY-layer. The success probability of the PHY layer was derived from the product of the characteristic function of the received power, Gaussian noise and aggregate interference. The probability of medium access, i.e. how many nodes will simultaneous transmit, is modeled through a Poisson distribution considering different network traffic loads. The impact of path loss and fading effects on the average number of successfully received frames is shown for different levels of network traffic load. Numerical and simulation results are used to evaluate the accuracy of the performance model, showing that it can be effectively used to anticipate an upper-bound of the performance when PHY-layer conditions are known in advance. The upper-bound is due to the fact that current LoRa receivers are unable to decode multiple frames at the same time. However, the results presented in the work clearly show the advantages of adopting receivers capable of decoding multiple frames simultaneously, which can effectively increase the capacity of future LoRa devices.

This work also studies LoRa's performance from the practical's viewpoint. A network

composed by a gateway and a single node is was deployed to assess the performance of LoRa communications in diverse scenarios. Through several tests which involved a node transmitting frames from different locations, empirical data was gathered. The data was used to characterize LoRa's performance in different propagation environments. Overall, it was shown that LoRa links are viable and can offer high performance in a variety of environments. Additionally, by comparing the results obtained in scenarios with and without line of sight, it was shown that dominant path of propagation between the node and gateway is much more determinative of the achievable performance, than the euclidean distance between the two.

6.2 Future Work

The theoretical performance model proposed in this thesis represents a departure point. Future iterations can extend the model to accommodate a network where the nodes use different spreading factors. There are several possible approaches to accomplish this. The network can be divided into annulus, where nodes inside each ring use a specific SF. Initially only two SFs can be considered as means to study the impact that inter spreading factor interference has on the probability of successful decoding a frame. Alternatively, nodes in the network can adopt a SF at random per transmission, to characterize the performance improvement or possibly decline brought by the adoption of an adaptive data rate. Considering only co-SF interference, most certainly the overall probability of success in the network will improve, since provided a network with the same number of nodes the average number of interfering signals will always be lower that the current model. Otherwise, i.e. considering inter-SF interference, the same can not be directly concluded, especially for scenarios with an higher node density or area radius. The model can also be adapted to derive the probability of successfully decoding a single frame given n_c concurrent transmissions. This can be done by identifying the dominant interferer signal and considering it as a successfully received frame if it holds a certain ratio relative to the remaining interfering signals, e.g. four times (6 dB) stronger, as mentioned in Section 4.2.

Regarding the practical evaluation of LoRa, there are a multitude of possible approaches. As a staring point, the measurements of performance can include scenarios with the gateway antenna positioned at different heights. More nodes can be added into the network in order to test the link performance under interference. Additionally, a general network server framework, which was not integrated into the LoRa network, was developed during the dissertation's work period. The network server features a java application connected to a MQTT broker (Eclipse Mosquitto) and a local postgreeSQL database. The intent was to connect the gateway to the aforementioned broker through a ssh connection. Messages received in the gateway would be forwarded to the broker. The java application would subscribe to the gateway specific topics and relay the messages to the postgreeSQL database. The NS is already capable of sending and receiving MQTT messages. However this component is not yet finished, as the topic structure was not defined. A simple file logger

and GUI (see Figures in Appendix A) were also developed to provide feedback and manage clients. Extending this network server and integrating it in the gateway in order to deploy an IoT network would constitute a more practical approach to continue with the practical assessment initiated in this dissertation.

Bibliography

[1] A. Abdi and M. Kaveh. "On the utility of gamma PDF in modeling shadow fading (slow fading)." In: (2003), pp. 2308–2312. DOI: 10.1109/vetec.1999.778479.

[2] Aegis Systems and Ovum Consulting. *Short Range Devices operating in the 863 - 870 MHz frequency band.* Tech. rep. August. Office of Communications (Ofcom), 2010. URL: https://www.ofcom.org.uk/{_}{_}data/assets/pdf{_}file/0025/38095/final{_}report.pdf.

[3] S. Al-Ahmadi and H. Yanikomeroglu. "On the approximation of the generalized-distribution by a gamma distribution for modeling composite fading channels." In: *IEEE Transactions on Wireless Communications* 9.2 (2010), pp. 706–713. ISSN: 15361276. DOI: 10.1109/TWC.2010.02.081266.

[4] A Al-Fuqaha, M Guizani, M. M. ... S. &. Tutorials, and undefined 2015. "Internet of things: A survey on enabling technologies, protocols, and applications." In: *Ieeexplore.Ieee.Org* 17.4 (2015), pp. 2347–2376. URL: http://ieeexplore.ieee.org/abstract/document/7123563/.

[5] M. Anteur, V. Deslandes, N. Thomas, and A. L. Beylot. "Ultra narrow band technique for low power wide area communications." In: *2015 IEEE Global Communications Conference, GLOBECOM 2015* (2015). DOI: 10.1109/GLOCOM.2014.7417420.

[6] A. Arsanjani. *Service-oriented modeling and architecture.* 2004. DOI: 10.1109/SCC.2006.93. URL: https://www.ibm.com/developerworks/library/ws-soa-design1/ (visited on 06/27/2018).

[7] K. Avila, P. Sanmartin, D. Jabba, and M. Jimeno. "Applications Based on Service-Oriented Architecture (SOA) in the Field of Home Healthcare." In: *Sensors* 17.8 (2017), p. 1703. ISSN: 1424-8220. DOI: 10.3390/s17081703. URL: http://www.mdpi.com/1424-8220/17/8/1703.

[8] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-c. Pr. "Internet of Mobile Things : Overview of LoRaWAN , DASH7 , and NB-IoT in LPWANs standards and Supported Mobility." In: April 2016 (2018). ISSN: 1553-877X. DOI: 10.1109/COMST.2018.2877382.

[9] M. C. Bor, U. Roedig, T. Voigt, and J. M. Alonso. "Do LoRa Low-Power Wide-Area Networks Scale?" In: *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems - MSWiM '16* November (2016), pp. 59–67. ISSN: 00404020. DOI: 10.1145/2988287.2989163. URL: http://dl.acm.org/citation.cfm?doid=2988287.2989163.

[10] C. Bormann, A. P. Castellani, and Z. Shelby. "CoAP: An application protocol for billions of tiny internet nodes." In: *IEEE Internet Computing* 16.2 (2012), pp. 62–67. ISSN: 10897801. DOI: 10.1109/MIC.2012.29.

[11] R. Chaâri, F. Ellouze, A. Koubâa, B. Qureshi, N. Pereira, H. Youssef, and E. Tovar. "Cyber-physical systems clouds: A survey." In: *Computer Networks* 108.September (2016), pp. 260–278. ISSN: 13891286. DOI: 10.1016/j.comnet.2016.08.017.

[12] M. Chen, Y. Miao, Y. Hao, and K. Hwang. "Narrow Band Internet of Things." In: *IEEE Access* 5 (2017), pp. 20557–20577. ISSN: 21693536. DOI: 10.1109/ACCESS.2017.2751586.

[13] R. Datasheet. "RisingHF DS01603 RisingHF." In: © *2016 RISINGHF - All rights reserved* (2016). URL: http://www.risinghf.com/.

[14] N. De Caro, W. Colitti, K. Steenhaut, G. Mangino, and G. Reali. "Comparison of two lightweight protocols for smartphone-based sensing." In: *IEEE SCVT 2013 - Proceedings of 20th IEEE Symposium on Communications and Vehicular Technology in the BeNeLux* (2013), pp. 0–5. ISSN: 2373-0854. DOI: 10.1109/SCVT.2013.6735994.

[15] C. P. Devi, M Sivaranjani, and V. P. Venkatesan. "Design of a Smart Gateway Solution Based on the Exploration of Specific Challenges in IoT." In: *International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017)* (2017), pp. 22–31. DOI: 10.1109/I-SMAC.2017.8058352.

[16] H. Factors. "Final draft ETSI EN 300 220-1 V2.4.1 (2012-01)." In: *Etsi* 0 (2014), pp. 1–73.

[17] J. Fakatselis. "Processing gain in spread spectrum signals." In: *Harris Semiconductor application note* (1998), pp. 1–5. ISSN: 0151-9638. DOI: 10.1016/j.annder.2007.02.001. URL: http://www.sss-mag.com/pdf/pgpap.pdf.

[18] A. P. Foster. "Messaging Technologies for the Industrial Internet and the Internet of Things." In: March (2014), pp. 1–22. URL: http://www.prismtech.com/sites/default/files/documents/MessagingComparsionMarch2014USROW-final.pdf.

[19] Frank W. J. Olver. *NIST Handbook of Mathematical Functions*. Vol. 5. Surf Iii. 1986. ISBN: 9780521140638.

[20] A. Furtado, S. Member, R. Oliveira, S. Member, R. Dinis, S. Member, and L. Bernardo. "Successful Packet Reception Analysis in Multi-Packet Reception Wireless Systems." In: 20.12 (2016), pp. 2498–2501. DOI: 10.1109/LCOMM.2016.2606105.

[21] J. Gantz and D. Reinsel. "T H E D I G I T AL U N I V E R S E I N 2 0 2 0 : B i g D a t a , Bigger Digital Shadows , and Biggest Growth in the Far East — United States." In: (2013), pp. 1–7.

[22] Gartner. *Real-Time Analytics - Gartner IT Glossary*. URL: https://www.gartner.com/it-glossary/real-time-analytics (visited on 06/15/2018).

[23] O. Georgiou and U. Raza. "Low Power Wide Area Network Analysis: Can LoRa Scale?" In: *IEEE Wireless Communications Letters* 6.2 (2017), pp. 162–165. ISSN: 21622345. DOI: 10.1109/LWC.2016.2647247. arXiv: 1610.04793.

[24] C. Goursaud and J. M. Gorce. "Dedicated networks for IoT: PHY / MAC state of the art and challenges." In: *EAI Endorsed Transactions on Internet of Things* 1.1 (2015), p. 150597. ISSN: 2414-1399. DOI: 10.4108/eai.26-10-2015.150597. arXiv: eai.26-10-2015.150597. URL: http://eudl.eu/doi/10.4108/eai.26-10-2015.150597.

[25] J. Gozalvez. "New 3GPP Standard for IoT [Mobile Radio]." In: *IEEE Vehicular Technology Magazine* 11.1 (2016), pp. 14–20. ISSN: 15566072. DOI: 10.1109/MVT.2015.2512358.

[26] I. Grigorik. "Making the web faster with HTTP 2.0." In: *Communications of the ACM* 56.12 (2013), pp. 42–49. ISSN: 00010782. DOI: 10.1145/2534706.2534721. URL: http://dl.acm.org/citation.cfm?doid=2534706.2534721.

[27] L. Guntupalli, R. Rondon, S. A. Hassan, M. Gidlund, E. Sisinni, and A. Mahmood. "Scalability Analysis of a LoRa Network under Imperfect Orthogonality." In: *IEEE Transactions on Industrial Informatics* August (2018), pp. 1–1. ISSN: 1551-3203. DOI: 10.1109/tii.2018.2864681.

[28] D. Hughes, P. Greenwood, G. Blair, G. Coulson, F. Pappenberger, P. Smith, and K. J. Beven. "An Intelligent and Adaptable Grid-based Flood Monitoring and Warning System." In: *Proceedings of the UK E-Science All Hands Meeting* (2006), pp. 53–60.

[29] IBM. *IBM Knowledge Center - Association rules*. URL: https://www.ibm.com/support/knowledgecenter/en/SS6NHC/com.ibm.swg.im.dashdb.analytics.doc/doc/r{_}association{_}rules.html (visited on 06/11/2018).

[30] C. Jakes. *Microwave Mobile Communications*. ISBN: 0780310691.

[31] R. Khan, S. U. Khan, R. Zaheer, and S. Khan. "Future internet: The internet of things architecture, possible applications and key challenges." In: *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012* (2012), pp. 257–260. ISSN: 1556-3669. DOI: 10.1109/FIT.2012.53. arXiv: 1207.0203.

[32] M. Knight and B. Seeber. "Decoding LoRa : Realizing a Modern LPWAN with SDR." In: *6th GNU Radio Conference* (2016), p. 5. URL: https://pubs.gnuradio.org/index.php/grcon/article/view/8.

[33] J. Lampe and Z. Ianelli. "Introduction to Chirp Spread Spectrum (CSS) Technology." In: November (2003), pp. 1–28. URL: https://www.google.co.uk/url?sa=t{\&}rct=j{\&}q={\&}esrc=s{\&}source=web{\&}cd=1{\&}cad=rja{\&}uact=8{\&}ved=0ahUKEwib396krNHJAhXCbRQKHTbSAJwQFgghMAA{\&}url=http{\%}3A{\%}2F{\%}2Fwww.ieee802.org{\%}2F802{_}tutorials{\%}2F03-November{\%}2F15-03-0460-00-0040-IEEE-802-CSS-Tutorial-part1.ppt{\&}usg=AFQjCNHZ1.

[34] D. J. Lewinski. "Nonstationary Probabilistic Target and Clutter Scattering Models." In: *IEEE Transactions on Antennas and Propagation* 31.3 (1983), pp. 490–498. ISSN: 15582221. DOI: 10.1109/TAP.1983.1143067.

[35] LoRa Alliance. *About LoRaWAN™ | LoRa Alliance™*. URL: https://lora-alliance.org/about-lorawan (visited on 11/26/2018).

[36] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa, and I. Yaqoob. "Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges." In: *IEEE Access* 5 (2017), pp. 5247–5261. ISSN: 21693536. DOI: 10.1109/ACCESS.2017.2689040. arXiv: 2017.

[37] G. Marsh, A. P. Sampat, S. Potluri, and D. K. Panda. "Scaling Advanced Message Queuing Protocol (AMQP) Architecture with Broker Federation and InfiniBand." In: *Topology* (2010). URL: http://scholar.google.com/scholar?hl=en{\&}btnG=Search{\&}q=intitle:Scaling+Advanced+Message+Queuing+Protocol+(AMQP)+Architecture+with+Broker+Federation+and+InfiniBand+?{\#}0.

[38] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer. "A comparative study of LPWAN technologies for large-scale IoT deployment." In: *ICT Express* (2018). ISSN: 24059595. DOI: 10.1016/j.icte.2017.12.005. URL: http://linkinghub.elsevier.com/retrieve/pii/S2405959517302953.

[39] K. Mikhaylov, J. Petäjäjärvi, and T. Hänninen. "Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology." In: *European Wireless 2016* May (2016), pp. 119–124.

[40] J Miranda, R Abrishambaf, T Gomes, P. Goncalves, J Cabral, A Tavares, and J Monteiro. "Path loss exponent analysis in Wireless Sensor Networks: Experimental evaluation." In: *2013 11th IEEE International Conference on Industrial Informatics (INDIN), Bochum, Germany* July (2013), pp. 54–58. ISSN: 19354576. DOI: 10.1109/INDIN.2013.6622857. URL: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6622857.

[41] H Mroue, A Nasser, B Parrein, S Hamrioui, and G Rouyer. "Analytical and Simulation study for LoRa Modulation." In: June (2018), pp. 655–659. DOI: 10.1109/ICT.2018.8464879.

[42] N. Naik. "Choice of Effective Messaging Protocols for IoT Systems : MQTT , CoAP , AMQP and HTTP." In: *2017 IEEE International Systems Engineering Symposium (ISSE)* (2017), pp. 1–7. DOI: 10.1109/SysEng.2017.8088251. URL: http://ieeexplore.ieee.org/document/8088251/.

[43] N. Naik and P. Jenkins. "Web protocols and challenges of Web latency in the Web of Things." In: *International Conference on Ubiquitous and Future Networks, ICUFN* 2016-Augus (2016), pp. 845–850. ISSN: 21658536. DOI: 10.1109/ICUFN.2016.7537156.

[44] C. L. Philip Chen and C. Y. Zhang. "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data." In: *Information Sciences* 275 (2014), pp. 314–347. ISSN: 00200255. DOI: 10.1016/j.ins.2014.01.015. arXiv: 1312.4722. URL: http://dx.doi.org/10.1016/j.ins.2014.01.015.

[45] Pluralsight. *Relational vs. non-relational databases: Which one is right for you? | Pluralsight*. URL: https://www.pluralsight.com/blog/software-development/relational-non-relational-databases (visited on 06/18/2018).

[46] N. Poursafar, M. E. E. Alahi, and S. Mukhopadhyay. "Long-range wireless technologies for IoT applications: A review." In: *Proceedings of the International Conference on Sensing Technology, ICST* 2017-Decem (2018), pp. 1–6. ISSN: 21568073. DOI: 10.1109/ICSensT.2017.8304507. URL: http://ieeexplore.ieee.org/document/8304507/.

[47] B. Reynders and S. Pollin. "Chirp spread spectrum as a modulation technique for long range communication." In: *2016 IEEE Symposium on Communications and Vehicular Technology in the Benelux, SCVT 2016* 2 (2016), pp. 0–4. DOI: 10.1109/SCVT.2016.7797659.

[48] A. P. Reynolds, G. Richards, B. De La Iglesia, and V. J. Rayward-Smith. "Clustering rules: A comparison of partitioning and hierarchical clustering algorithms." In: *Journal of Mathematical Modelling and Algorithms* 5.4 (2006), pp. 475–504. ISSN: 15701166. DOI: 10.1007/s10852-005-9022-1.

[49] Risinghf. "RisingHF UM01509 RisingHF." In: (2016), p. 44. URL: https://fccid.io/2AJUZ76052/User-Manual/Users-Manual-3211050.

[50] I. M. Ruizhik, Y. V. Geronimus, M. Y. Tseytlin, and A. Jeffrey. *Table of integrals, series, and products. (Tablitsy integralov, summ ...* 1965, p. 1086. ISBN: 0080471110. DOI: 10.1017/CBO9781107415324.004. arXiv: arXiv:1011.1669v3.

[51] H. Saadeh, W. Almobaideen, and K. E. Sabri. "Internet of Things: A review to support IoT architecture's design." In: *2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS)*. IEEE, 2017, pp. 1–7. ISBN: 978-1-5386-1984-1. DOI: 10.1109/IT-DREPS.2017.8277803. URL: http://ieeexplore.ieee.org/document/8277803/.

[52] C. Sarkar, A. U. Akshay, R. V. Prasad, A. Rahim, R. Neisse, and G. Baldini. "DIAT: A scalable distributed architecture for IoT." In: *IEEE Internet of Things Journal* 2.3 (2015), pp. 230–239. ISSN: 23274662. DOI: 10.1109/JIOT.2014.2387155.

[53] M. Schwartz. *Mobile Wireless Communications*. Cambridge University Press, New York, 2005, p. 457. ISBN: 9780521843478. DOI: 10.1017/cbo9780511811333.003.

[54] *Seeeduino LoRaWAN - Seeed Wiki*. URL: http://wiki.seeedstudio.com/Seeeduino{_}LoRAWAN/ (visited on 03/22/2019).

[55] O. B. A. Seller and N. Sornin. *Low power long range transmitter*. 2014. URL: https://patents.google.com/patent/EP2763321A1/en.

[56] Semtech. "LoRa Modem Design Guide." In: July (2013), pp. 1–9. DOI: 10.1108/03090561211202602. URL: http://www.semtech.com/images/datasheet/LoraDesignGuide{_}STD.pdf.

[57] Semtech. *AN1200.22 LoRa Modulation Basics*. 2015. URL: http://www.semtech.com/images/datasheet/an1200.22.pdf.

[58] Semtech. *SX1272/73 - 860 MHz to 1020 MHz Low Power Long Range Transceiver*. 2017. URL: https://www.semtech.com/uploads/documents/SX1272{_}DS{_}V4.pdf.

[59] Semtech. *WIRELESS & SENSING PRODUCTS Datasheet SX1301*. 2017. URL: https://www.semtech.com/uploads/documents/sx1301.pdf.

[60] E. Serrano and A. Arsénio. "Cloud Framework for Wireless Sensor Networks." Lisboa, 2009. URL: https://fenix.tecnico.ulisboa.pt/downloadFile/281870113702070/DissertacaoResumo-EduardoSerrano-56879.pdf.

[61] B. Server. *Introduction to Bayesian networks*. URL: https://www.bayesserver.com/docs/introduction/bayesian-networks (visited on 06/08/2018).

[62] P. Sethi and S. R. Sarangi. "Internet of Things: Architectures, Protocols, and Applications." In: *Journal of Electrical and Computer Engineering* 2017 (2017). ISSN: 20900155. DOI: 10.1155/2017/9324035.

[63] W. Shang, Y. Yu, L. Zhang, and R. Droms. "Challenges in IoT Networking via TCP/IP Architecture." In: *NDN Project, Tech. Rep. NDN-0038* 8.2 (2016), p. 7. URL: http://named-data.net/wp-content/uploads/2016/02/ndn-0038-1-challenges-iot.pdf.

[64] Sigfox. *Coverage | Sigfox*. URL: https://www.sigfox.com/en/coverage (visited on 04/25/2018).

[65] Sigfox. "Sigfox Technical Overview." In: 1.May (2017), p. 26. URL: https://www.disk91.com/wp-content/uploads/2017/05/4967675830228422064.pdf.

[66] R. S. Sinha, Y. Wei, and S. H. Hwang. "A survey on LPWA technology: LoRa and NB-IoT." In: *ICT Express* 3.1 (2017), pp. 14–21. ISSN: 24059595. DOI: 10.1016/j.icte.2017.03.004. URL: http://dx.doi.org/10.1016/j.icte.2017.03.004.

[67] N. Sornin (Semtech), M. Luis (Semtech), T. Eirich (IBM), T. Kramp (IBM), and O. Hersent (Actility). *LoRaWAN Specification V1.0*. 2015. URL: https://lora-alliance.org/resource-hub/lorawanr-specification-v10.

[68] A. Stanciu, T. C. Balan, C. Gerigan, and S. Zamfir. "Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm." In: *Proceedings - 2017 International Conference on Optimization of Electrical and Electronic Equipment, OPTIM 2017 and 2017 Intl Aegean Conference on Electrical Machines and Power Electronics, ACEMP 2017* (2017), pp. 1001–1006. DOI: 10.1109/OPTIM.2017.7975101.

[69] G. L. Stüber. *Principles of Mobile Communication*. New York, NY: Springer New York, 2012. ISBN: 978-1-4614-0363-0. DOI: 10.1007/978-1-4614-0364-7. URL: http://link.springer.com/10.1007/978-1-4614-0364-7.

[70] G. Suciu, S. Halunga, A. Vulpe, and V. Suciu. "Generic platform for IoT and cloud computing interoperability study." In: *ISSCS 2013 - International Symposium on Signals, Circuits and Systems* (2013). ISSN: 9781479931934. DOI: 10.1109/ISSCS.2013.6651222.

[71] A. S. Tanenbaum. *Computer Networks*. Vol. 52. 169. 1996, pp. 349–351. ISBN: 0130661023. DOI: 10.1016/j.comnet.2008.04.002. arXiv: 1011.1529. URL: http://www.ietf.org/rfc/rfc169.txt.

[72] S. Tilkov. "Semantic Gateway as a Service architecture for IoT Interoperability." In: *IEEE Software* 32.2 (2015). ISSN: 07407459. DOI: 10.1109/MS.2015.51.

[73] S. Whitening. "Implementing Data Whitening and CRC Calculation in Software on SX12xx Devices Table of Contents Index of Figures." In: October (2013), pp. 1–14.

[74] N. A. B. Zainal, M. H. Habaebi, I. Chowdhury, and M. R. Islam. "Sensor node clutter distribution in LoRa LPWAN." In: *2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA)* November (2017), pp. 1–6. DOI: 10.1109/ICSIMA.2017.8312013. URL: http://ieeexplore.ieee.org/document/8312013/.

[75] Z. Zheng, R. Kohavi, and L. Mason. "Real world performance of association rule algorithms." In: *Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '01* (2001), pp. 401–406. DOI: 10.1145/502512.502572. URL: http://portal.acm.org/citation.cfm?doid=502512.502572.

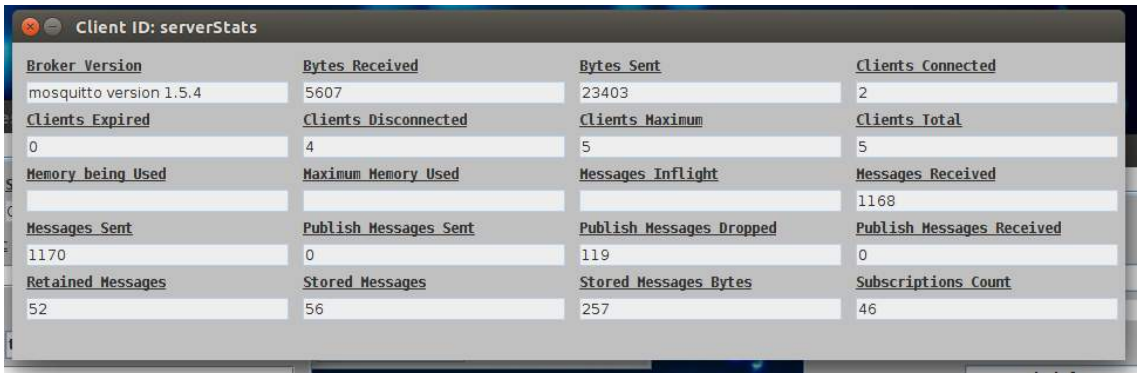
[76] Zhihong Yang, Yufeng Peng, Yingzhao Yue, Xiaobo Wang, Yu Yang, and Wenji Liu. "Study and application on the architecture and key technologies for IOT." In: *2011 International Conference on Multimedia Technology* (2011), pp. 747–751. DOI: 10.1109/ICMT.2011.6002149. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6002149.

[77] O. Zimmermann, P. Krogdahl, and C. Gee. *Elements of Service-Oriented Analysis and Design.* URL: https://www.ibm.com/developerworks/library/ws-soad1/index.html (visited on 06/27/2018).

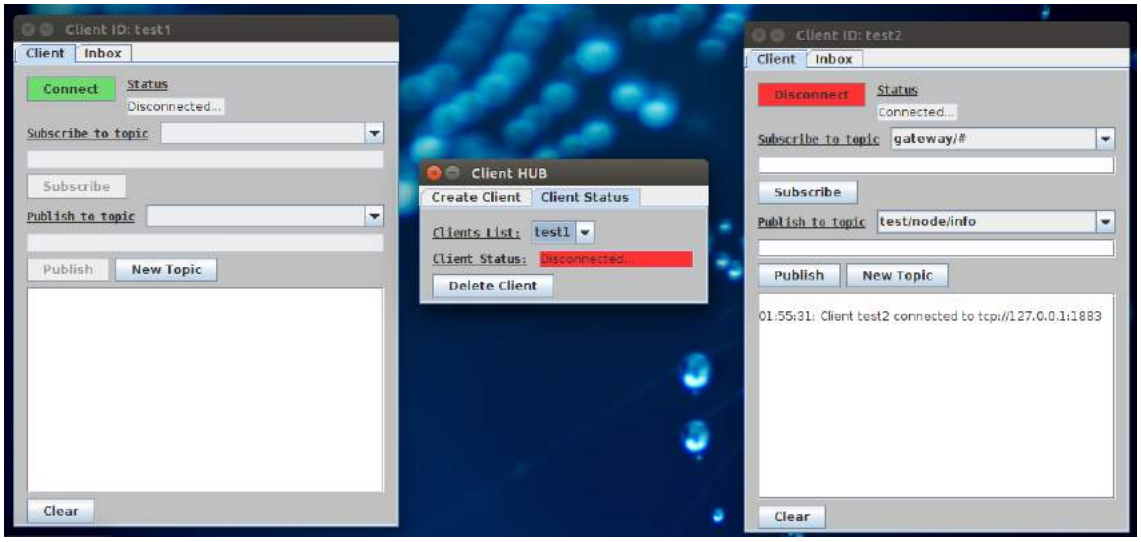
[78] D. Zwillinger. *CRC Standard Mathematical Tables and Formulas 33rd Edition.* CRC Press, 2017, p. 873. ISBN: 9781498777803.

APPENDIX A

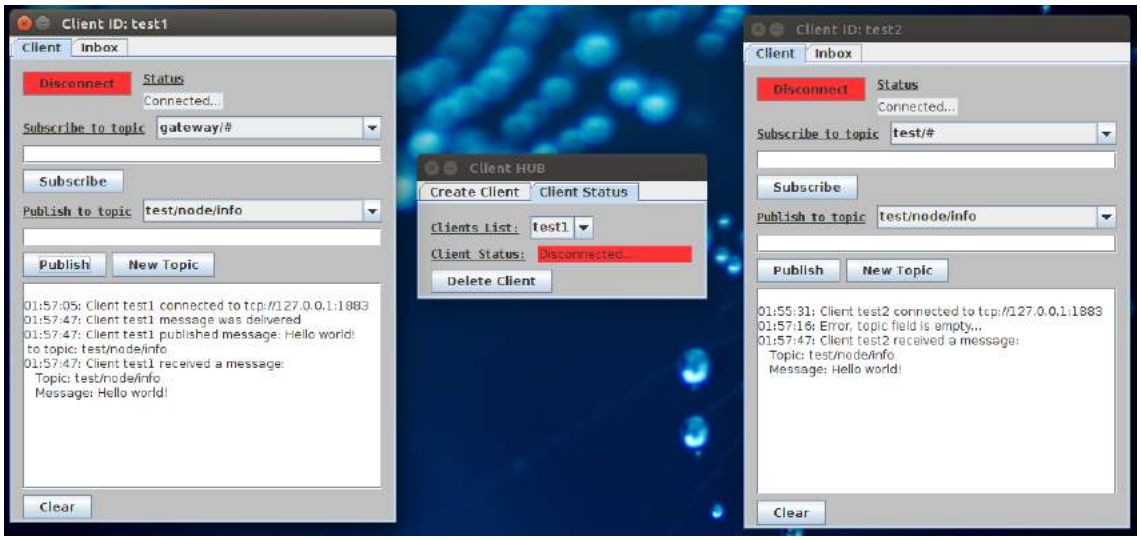
Network Server GUI



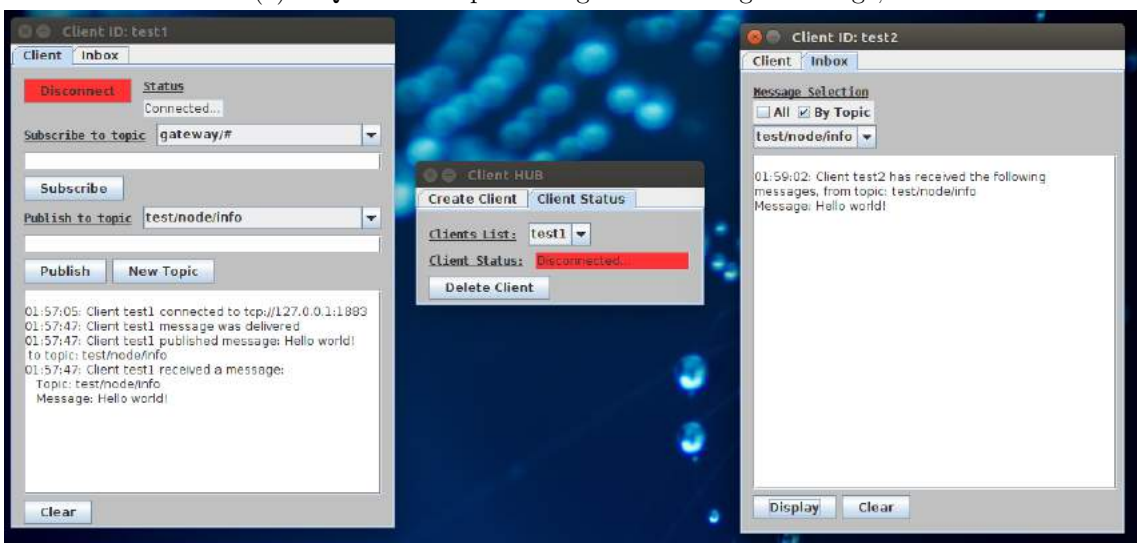
(a) MQTT Broker statistics;



(b) MQTT client and client creator GUIs;



(a) MQTT clients publishing and receiving a message;



(b) MQTT client message inbox;

ANNEX I

Submitted Conference Paper

PHY/MAC Uplink Performance of Class A LoRa Networks

João Pacheco*, António Furtado†, and Rodolfo Oliveira*†

*Departamento de Engenharia Electrotécnica, Faculdade de Ciências e Tecnologia (FCT),
Universidade Nova de Lisboa, Caparica, Portugal
†IT, Instituto de Telecomunicações, Portugal

***Abstract*—Recently, Low Power Wide Area Networks (LPWANs) have attracted a great interest due to the need of connecting more and more devices to the so-called Internet of Things (IoT). LoRa networks are LPWANs that allow a long-range radio connection of multiple devices operating in non-licensed bands. In this work, we characterize the performance of LoRa's Uplink communications where both physical layer (PHY) and medium access control (MAC) are taken into account. By admitting a uniform spatial distribution of the devices, we characterize the performance of the PHY-layer through the probability of successfully decoding multiple frames that were transmitted with the same spreading factor and at the same time. The MAC performance is evaluated by admitting that the inter-arrival time of the frames generated by each LoRa device is exponentially distributed. A typical LoRaWAN operating scenario is considered, where the transmissions of LoRa Class A devices are affected by path-loss, shadowing and Rayleigh fading. Numerical results obtained with the modeling methodology are compared with simulation results, and the validation of the proposed model is discussed for different levels of traffic load and PHY-layer conditions. Due to the possibility of capturing multiple frames simultaneously, we consider the maximum achievable performance of the PHY/MAC LoRa scheme according to the Signal-to-interference-plus-noise ratio (SINR). The contribution of this work is primarily focused on studying the average number of successfully received LoRa frames, which establishes a performance upper bound due to the optimal capture condition considered in the PHY-layer.**

***Index Terms*—LoRa Networks, PHY/MAC Modeling, Performance Evaluation.**

I. Introduction

Nowadays billions of devices are being connected to the so-called Internet of Things (IoT), having motivated several standardization initiatives and proprietary protocols capable of supporting a massive number of radio connected devices. Although the high number of radio access technologies already available to support wideband data communications (e.g. WiFi, GPRS, 3G, 4G, etc.), it is widely agreed that radio access to IoT networks requires specific protocols particularly tailored to support a massive number of nodes that may be deployed as necessary. To support IoT devices the radio access networks require new features including: (i) the adoption of devices that operate with very low power in order to minimize energy consumption; (ii) long-range radio links to cover wide areas; (iii) massive connectivity support of devices requiring a few tens of kilobits per second. The response to these requirements has been given by the so called Low Power Wide Area Networks (LPWANs) [1], capable of offering affordable low-power devices that operate over very large geographical areas. Contrarily to short-range wireless protocols already proposed for IoT radio access, e.g., Bluetooth, IEEE 802.15.4, LPWANs support long range and low-power operation to a high number of connected devices at the expense of slowing down the transmission rate and increasing latency. Several LPWA technologies have already been proposed. Traditional cellular network operators are currently offering commercial LPWA technologies in licensed bands, e.g. LTE enhancements for Machine Type Communications (eMTC), Extended Coverage GSM (EC-GSM), and Narrow-Band IoT (NB-IoT). Simultaneously, proprietary LPWA technologies, e.g. Sigfox, LoRa, and Ingenu, have gaining interest due to the lower operational costs in non-licensed bands and because they can be deployed at certain areas where no cellular operators are available. In this work we are particularly focused on study LoRa's performance due to the rising interest of practitioners, who are currently deploying a global open LoRaWAN network through personal gateways that enable LoRa devices to connect to a decentralized network to exchange data with the applications [2].

LoRa is a proprietary physical layer technology, developed by Semtech Corporation [3], that uses a chirp spread spectrum technique to spread a narrow band signal over a 125, 250 or 500 kHz bandwidth located in a sub-gigahertz unlicensed ISM band. This allows the receiver, usually a gateway, to decode signals a few dBs below the noise floor. The transmission range and the data rate can be also controlled through different Spreading Factors (SF), which vary the receivers' sensitivity threshold. LoRaWAN [4] is a medium access control (MAC) protocol designed to run on top of LoRa's modulation. LoRaWAN offers bidirectional communications initiated by the receiver. The communication is initiated by a LoRa device, which sends an uplink message in a random access mode (similar to ALOHA). A LoRa gateway can then respond to the device if the uplink message is successfully received. The devices supporting the bidirectional communication scheme is designated Class A devices.

The remainder of this paper is organized as follows. Next we discuss the related work and the contributions of this work. Section II presents the LoRa network scenario. Section III

describes the steps involved to model the performance related with LoRa's PHY/MAC design. Section IV compares and analyzes different numerical and simulation results. Finally, conclusions are presented in Section V.

Notations: In this work, $f_X(.)$ represents the Probability Density Function (PDF) of a random variable (RV) X. P$[X = x]$ and E$[X]$ represent the probability and the expectation of the RV X, respectively.

A. Related Work

The performance of LoRa networks has attracted an increasing interest [5]–[11]. Real world indoor and outdoor evaluation campaigns were presented in [5] and [6], respectively. The work in [7] has characterized the capture condition when multiple frames collide. When multiple LoRa frames are simultaneously received using the same Spreading Factor the weaker signals can be suppressed by the strongest ones and the receiver can decode a frame involved in a collision. This is against the traditional collision model, where all frames involved in a collision are considered lost. [8] defined a threshold-based power condition for capture occurrence when two LoRa frames are transmitted. When two frames are simultaneously received [8] reports that the strongest one can be successfully received if its power is at least 6 dB above the weaker signal. However, this is not confirmed in [9], where small-scale experimental results lead to a difference of 15 dB (far above the 6 dB threshold). [9] also investigated the impact of the transmission timings (time offset between the beginning of colliding frames) on the capture effect, showing that the capture of a single frame only occurs in specific time offset values.

LoRa's scalability was addressed in [10], by considering two capture conditions for the uplink messages. The first condition was based on the received Signal-to-Noise Ratio (SNR), while the second one assumed that the uplink message is successfully received whenever its power is approximately 4 times (6 dB) higher than any concurrent transmission. Based on the second capture condition [10] concludes that the interference caused by concurrent uplink transmissions can effectively limit the scalability of LoRa networks. While [10] considers that LoRa devices adopt the same SF, [11] evaluates the throughput when concurrent upload messages are transmitted with different spreading factors. Admitting that a few LoRa devices may use the same SF and the remaining ones can adopt different SFs, [11] derives the network's throughput for different types of SF allocations.

B. Contributions

Motivated by the importance of LoRa networks, this work characterizes the performance of the PHY/MAC uplink by studying the average of frames that are successfully decoded by the LoRa gateway. Our work adopts a typical LoRaWAN operating scenario, where LoRa Class A devices transmit with a given probability and are affected by path-loss, shadowing and Rayleigh fading. The contributions of this work are summarized as follows:

1) Differently from the works in [7]–[11], in this paper we consider a PHY-layer SINR-based capture condition. Consequently, we assume that multiple frames can be successfully received at the same time, which can be viewed as an upper bound of the PHY-layer performance;
2) LoRa's Class A uplink MAC protocol is considered, and the number of devices involved in a collision is modeled and validated for exponential traffic sources;
3) Joint PHY/MAC performance is studied through the average number of successfully decoded frames for different levels of network load and physical-layer conditions;
4) Numerical and simulation results are compared to evaluate the accuracy of the performance analysis.

To the best of the authors' knowledge, the presented results are new and can definitely be used as a benchmark for future LoRa performance evaluation.

II. LoRa Network

We consider a LoRa network scenario where n devices are distributed over a circular region of radius R centered at the gateway. The LoRa devices are spatially positioned according to a uniform distribution in $\mathbb{R}^2$, with spatial density $\sigma = \frac{n}{\pi R^2}$. The work considers the uplink of Class A devices, where nodes adopt the Aloha protocol. Each device transmits a frame with probability τ.

Regarding the assumptions related with the radio propagation, we consider that the fading between each device and the gateway is independent and identically distributed (i.i.d). The gain due to path-loss is equal to [12] $(\frac{w}{d_k+1})^{-\alpha}, d_k \in [0, R]$, where the RV d_k represents the euclidean distance between the LoRa device and the gateway, and w is given by $\frac{c}{4\pi f_c}$, where c is the speed of light and f_c is the carrier frequency. α represents the path loss coefficient. Rayleigh fading and Lognormal shadowing is assumed. The fast fading gain is assumed to be distributed according to a Rayleigh distribution with PDF

$$f_\zeta(x) = \frac{x}{\sigma_\zeta^2} e^{\frac{-x^2}{2\sigma_\zeta^2}}, \tag{1}$$

where $2\sigma_\zeta^2$ is the average gain (we consider normalized gain, i.e., $2\sigma_\zeta^2 = 1$). The shadowing gain is approximated by a Lognormal distribution

$$f_\xi(x) = \frac{1}{\sqrt{2\pi}\sigma_\xi x} e^{\frac{-(ln(x)-\mu_\xi)^2}{2\sigma_\xi^2}}, \tag{2}$$

where $\sigma_\xi > 0$ and $\mu_\xi = -\frac{\sigma_\xi^2}{2}$ to consider average unitary gain. However, due to the mathematical intractability of Lognormal RVs we use a Gamma distribution given by

$$f_\xi(x) \approx \frac{1}{\Gamma(\vartheta)} \left(\frac{\vartheta}{\omega_s}\right)^\vartheta x^{\vartheta-1} e^{-x\frac{\vartheta}{\omega_s}}, \tag{3}$$

with $\vartheta = \frac{1}{e^{\sigma_\xi^2}-1}$ and $\omega_s = e^{\mu_\xi}\sqrt{\frac{\vartheta+1}{\vartheta}}$, which can be used to replace the Lognormal distribution is an accurate manner [13].

Finally, the PDF of the fading and shadowing power gain is given by $f_{\Psi_i}(x) \approx f_{\zeta^2}(x) \cdot f_{\xi}(x)$, where the RV Ψ_i represents the joint effect (small-scale fading and shadowing). After a few algebraic steps, $f_{\Psi_i}(x)$ can be simplified to

$$f_{\Psi_i}(x) \approx \frac{2x^{\frac{\vartheta-1}{2}}}{\Gamma(\vartheta)} \left(\frac{\vartheta}{\omega_s}\right)^{\frac{\vartheta+1}{2}} K_{\vartheta-1}\left(\sqrt{\frac{4\vartheta x}{\omega_s}}\right). \quad (4)$$

(4) is the PDF of a Generalized-K distribution [14], which can be approximated by a Gamma distribution with scale and shape parameters given by $\theta_\psi = \left(\frac{2(\vartheta+1)}{\vartheta} - 1\right)\omega_s$ and $k_\psi = \frac{1}{\frac{2(\vartheta+1)}{\vartheta}-1}$, respectively [15].

III. PHY/MAC Model

A. Medium Access Control

Each one of the n LoRa devices competing in the uplink of the network generates frames with inter-arrival time exponentially distributed with average λ^{-1} time units per frame. The PDF of the frames inter-arrival time is represented by

$$f_I(x) = \lambda e^{-\lambda x}. \quad (5)$$

LoRa devices adopt the $Aloha$ protocol, meaning that a device starts a new transmission whenever it has a new frame to send[1]. Each node transmits a frame with probability

$$\tau = \begin{cases} \lambda, & 0 \leq \lambda \leq 1 \\ 1, & \lambda > 1. \end{cases}$$

Due to the distribution of the inter-arrival times, the number of frames generated by n nodes per time unit is represented by the random variable K, distributed according to a truncated Poisson distribution as follows

$$f_K(k) = \frac{e^{-n\lambda}(n\lambda)^k}{k!} \left(\sum_{m=0}^{n} \frac{(n\lambda)^m e^{-(n\lambda)}}{m!}\right)^{-1}, k = 0, ..., n. \quad (6)$$

From (6), the probability of observing a transmission in a given time unit is given by $1 - f_K(0)$. Representing the number of devices involved in a transmission by the RV C, the probability of observing c devices transmitting in a concurrent way is given by

$$\mathrm{P}[C = c] = \frac{f_K(c)}{1 - f_K(0)}, c = 1, ..., n. \quad (7)$$

We highlight that for $\mathrm{P}[C = c]$ also represents the probability of the number of devices participating in a collision when $c > 1$. Finally, the total load generated by the n devices is represented by $G = n\lambda$.

[1]In this work we assume that the probability of a device generating more than a single frame per time unit is approximately zero. This is a reasonable assumption for LoRa devices due to the low transmission rate and low duty cycle imposed by the regulatory bodies (less than 1% or 10% of spectrum usage, depending on the operating bands).

B. Physical Layer

In this subsection we consider that $1 \leq n_c \leq n$ nodes transmit data simultaneously to the LoRa gateway. We start to consider that the signals received from the LoRa devices are i.i.d. RVs, characterized by the PDF f_{P_k}. The aggregate power received in the gateway from the LoRa devices is given by

$$\Xi = \sum_{k=1}^{n_c} P_k + N_0, \quad (8)$$

where P_k is a RV representing the power received by the gateway from the k-th LoRa device and N_0 is a RV that represents the Additive White Gaussian Noise (AWGN) power at the gateway, with zero mean and variance [16] $\nu = -174 + NF + 10\log_{10} BW$ dB, where NF is the receiver hardware specific noise figure and BW is the bandwidth. In this work we consider that the LoRa gateway can receive multiple frames transmitted with the same Spreading Factor. To this end we consider the SINR associated to the transmission of a generic device j,

$$\gamma_j = P_j/(\Xi - P_j), \quad (9)$$

and the capture condition for each concurrent transmission j is defined as

$$\gamma_j > b. \quad (10)$$

In (10) the parameter b represents the LoRa Spreading Factor (SF) specific threshold [10], which represents the minimum SINR value above which a frame can be successfully decoded. We are now interested in deriving the probability of decoding an individual frame at the gateway. From (10), the successful decoding of a single frame implies the observation of the following condition

$$P_j > \frac{b}{b+1}\Xi, \quad (11)$$

and the probability of successfully receiving a frame can be written as follows

$$\mathrm{P}[S|n_c] = 1 - \mathrm{P}[P_j - \frac{b}{b+1}\Xi \leq 0]. \quad (12)$$

By considering a RV $\Upsilon = P_j - \frac{b}{b+1}\left(\sum_{k=1}^{n_c} P_k + N_0\right)$, we can write the characteristic function of Υ as follows

$$\varphi_\Upsilon(t) = \varphi_{P_j}\left(\frac{t}{b+1}\right) \cdot \prod_{k=1, k\neq j}^{n_c} \varphi_{P_k}\left(-\frac{b}{b+1}t\right) \cdot \varphi_{N_0}\left(-\frac{b}{b+1}t\right), \quad (13)$$

where φ_{N_0} represents the characteristic function of the noise. Because Zero-mean AWGN is assumed, $\varphi_{N_0}(t) = \frac{\sigma^2_{N_0}}{\sigma^2_{N_0} + it}$, where $\sigma^2_{N_0}$ is given by $10^{\frac{\nu}{10}}$. Regarding φ_{P_j} and φ_{P_k}, they represent the characteristic function of the frame's power to be decoded and the power of the interfering frames, being

derived with the methodology presented in [17], and written as

$$\varphi_{P_j}(t) = \varphi_{P_k}(t) = \frac{2}{R^2(-itwP_T\theta_\psi)^{k_\psi}} \cdot \cdot \left[\frac{\mathbb{I}_1(1) - (1+R)^{1+\alpha k_\psi}\mathbb{I}_1\left((1+R)^\alpha\right)}{1+\alpha k_\psi} + + \frac{(1+R)^{2+\alpha k_\psi}\mathbb{I}_2\left((1+R)^\alpha\right) - \mathbb{I}_2(1)}{2+\alpha k_\psi} \right], \quad (14)$$

where $\mathbb{I}_m(z) = {}_2\mathrm{F}_1\left(k_\psi, k_\psi + \frac{m}{\alpha}, 1 + k_\psi + \frac{m}{\alpha}, -\frac{iz}{twP_T\theta_\psi}\right)$, ${}_2\mathrm{F}_1$ represents the the Gauss Hypergeometric function [18, eq. 15.2.1], and P_T represents the transmission power adopted by the LoRa devices.

From (12) and using (14), the probability of successful frame reception can now be written as

$$\mathrm{P}[S|n_c] = 1 - \frac{1}{2\pi}\int_{-\infty}^{0} \mathrm{e}^{-ixt}\varphi_{P_j}\left(\frac{t}{b+1}\right)\cdot\varphi_{N_0}\left(-\frac{b}{b+1}t\right) \left(\varphi_{P_k}\left(-\frac{b}{b+1}t\right)\right)^{n_c-1} \mathrm{d}x, \quad (15)$$

which can be easily computed through the Fast Fourier Transform (FTT) algorithm.

C. Joint PHY/MAC Performance

When $1 \leq n_c \leq n$ nodes collide the probability of a LoRa gateway successfully decoding a frame can be easily computed through (15), which considers the PHY-layer propagation effects (k_ψ, θ_ψ, α), the devices' transmitting power (P_T), and the area of the circular region where the nodes are located (R). However, when the MAC is considered the number of devices involved in a collision (n_c) is a time-varying variable.

The probability of successfully decoding a frame when n nodes compete is given by

$$\mathrm{P}[S] = \frac{\sum_{k=1}^{n} k\ \mathrm{P}[S|k]\ \mathrm{P}[C=k]}{\sum_{k=1}^{n} k\ \mathrm{P}[C=k]}, \quad (16)$$

where $\mathrm{P}[C=k]$ is the information from the MAC layer in (7) and $\mathrm{P}[S|k]$ represents the probability of success at the PHY-layer in (15). Because in this work we have considered that the power received in the gateway from each LoRa device is i.i.d., the number of frames successfully and simultaneously received at the gateway can be approximated by

$$\mathrm{E}[N_{rx}] \approx \sum_{k=1}^{n} k\ \mathrm{P}[S|k]\ \mathrm{P}[C=k]. \quad (17)$$

IV. Performance Evaluation

In this Section we evaluate the accuracy of the performance model by comparing numerical and simulated results. LoRa's uplink performance is also analyzed for different propagation and traffic load scenarios.

Regarding the LoRa network scenario considered in the performance evaluation, and unless otherwise stated, we have considered a circular region with a radius $R = 1$ Km centered at the gateway. The network is operating at 868 MHz, occupying a bandwidth of 125 kHz. All devices adopt the same spreading factor (SF = 7) and transmission power ($P_T = 14$ dBm). The capture threshold was parameterized to $b = -6$ dBm [19], which allows the capture of multiple frames at the same time. Regarding the traffic model, we have considered each time unit equal to the frame's duration. The parameters adopted in the performance evaluation are presented in Table I.

TABLE I
Parameters adopted in the performance analysis.

P_T	14 dBm	f_c	868 MHz
σ_ζ^2	0.5	BW	125 kHz
λ	0.1 frames/time unit/device	R	1 km
NF	6 dB	Number of trials	10^5 simulations
b	-6 dBm	SF	7
α	2.01	σ_ξ	0.69

First we characterize the MAC behavior when $n = 10$ LoRa devices compete. Numerical results obtained with (7) are plotted in Figure 1, representing the probability of the number of competing nodes (c). The load generated by $n = 10$ LoRa devices, $G = n\lambda$, was changed from 0.1 to 10 frames per time unit, varying λ from 0.01 to 1 frames per time unit per device. For sake of simplicity we considered that a time unit is equal to the duration of each frame (all nodes adopt the same frame length). Usually LoRa networks operate in the unsaturated traffic region, i.e., $G \leq 1$. For $G \leq 1$ we observe that the probability of having a single device accessing the medium ($c = 1$) is always greater than 0.5. As

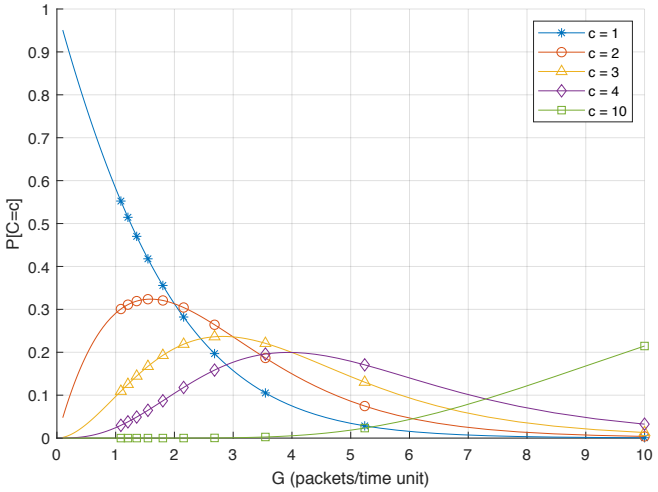
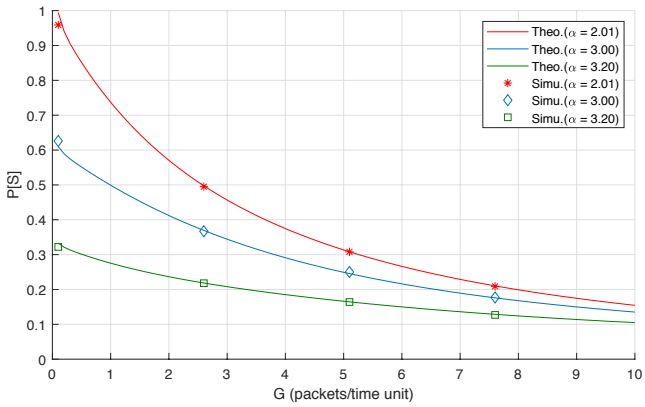
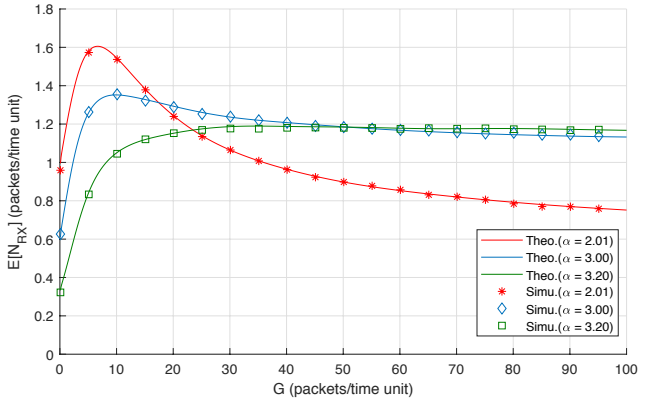


Fig. 1. Probability of observing $c = 1, 2, 3, 4, 10$ concurrent transmissions.

G increases from 0 to 1 the probability of only transmitting a single device decreases, but the probabilities of observing a

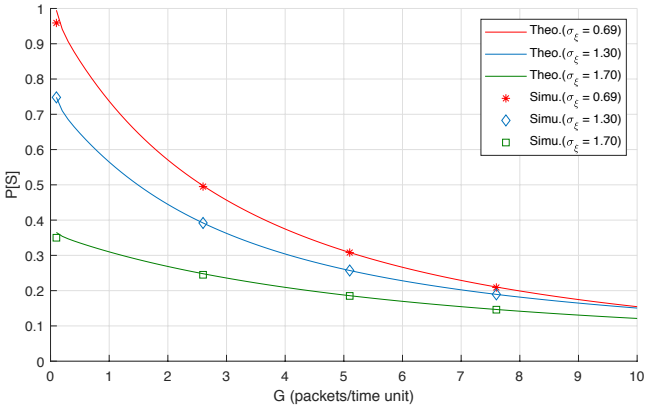


(a)

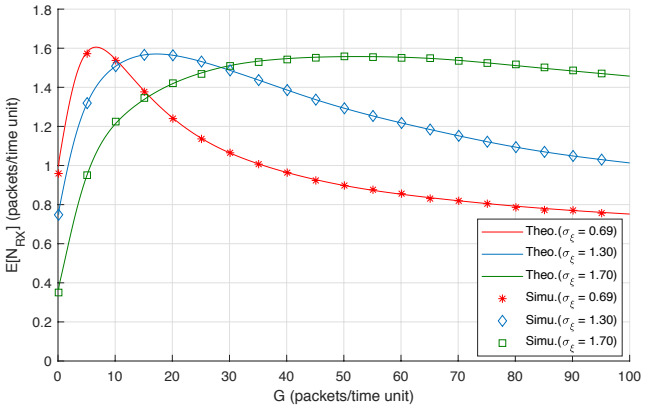


(b)

Fig. 2. (a) Successful frame reception probability (P[S]) for different path loss scenarios, α; (b) Average number of successful received frames (E[N_{rx}]) for different path loss scenarios, α.



(a)



(b)

Fig. 3. (a) Successful frame reception probability (P[S]) for different shadowing scenarios, σ_ξ; (b) Average number of successful received frames (E[N_{rx}]) for different shadowing scenarios, σ_ξ.

collision between $c = \{2, 3, 4, 10\}$ devices increase. However, for $G \approx 1$ frames per time unit the probability of observing collisions involving 4 frames is close to zero, meaning that the occurrence of collisions involving 5 or more devices can be neglected for $G \leq 1$.

In Figure IV we compare numerical and simulated results. The results were obtained for the same scenario, where the number of devices, n, was changed from 1 to 1000 nodes and we have considered that each device generates an average of $\lambda = 0.1$ frames/time unit. The multiple curves represent the performance for different path loss coefficients, α, and Rayleigh fading was parameterized with $\sigma_\xi = 0.69$. The numerical results are represented by the solid lines, while the simulation results are represented by the markers. The simulation results represent the average of 10^5 simulations. In Figure 2(a) we plot the probability of receiving an individual frame at the gateway, P[S], and the numerical results were computed using (16). Figure 2(b) plots the expected number of successful frames received at the gateway, E[N_{rx}], and the numerical results were computed with (17). For both P[S] and E[N_{rx}] we observe that the numerical results are close to the simulation results, showing the accuracy of the performance model proposed in this work. P[S] decreases as the network load increase and lower P[S] values are observed for higher path loss coefficients. E[N_{rx}] achieves a maximum that depends on the path loss coefficient. As depicted in Figure 2(b), more frames can be successfully received for lower path loss coefficients.

In Figure 3 we also characterize P[S] and E[N_{rx}]. However, the results were obtained for a constant path loss coefficient ($\alpha = 2.01$) and we assess the impact of the fading by considering different fading uncertainty (the fading uncertainty increases with σ_ξ). As can be seen in Figure 3(a), the probability of successfully receiving a frame decreases as the fading uncertainty increases. Regarding E[N_{rx}], we observe that higher fading uncertainty move the optimal point of operation to the right, meaning that the increase of fading uncertainty can only be compensated through the increase of the network's traffic load. Once again, the simulation results are close to the numerical results, confirming the accuracy of the proposed model.

In Figure 4 we study the impact of of the different spreading factors considering the same scenario of Figure (for $\alpha = 2.01$ and $\sigma_\xi = 0.69$). The curves in the figure represent the cases when the spreading factor 7, 8, 9, 10, 11, and 12 are adopted by the nodes and the gateway, which correspond to $b = \{-6, -9, -12, -15, -17.5, 20\}$ dB [19], respectively. As the spreading factor increases, b decreases and, consequently, the average number of successfully received frames increase. The curves confirm that higher spreading factors allow more frames to be successfully decoded at the same time. The average number of frames successfully received also vary with the network's load, and has a maximum for all considered spreading factors. Finally, we have included a curve for $b = 0$ dB. Although $b = 0$ dB does not represent any spreading factor adopted by LoRa, we have included it for comparison purposes, because it represents the case when only a single frame is captured at a given time instant. By comparing the curve for b =0 dB with the other curves, we are able to highlight the gain of adopting a multi-capture receiver when compared to the case when at most a single frame is received.

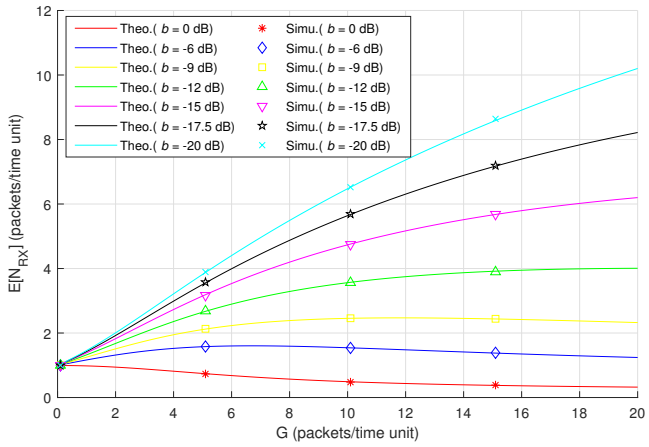


Fig. 4. Average number of received frames ($\mathrm{E}[N_{rx}]$) for different values of b (for $\alpha = 2.01$ and $\sigma_\xi = 0.69$).

V. Conclusions

This work adopts a typical LoRaWAN operating scenario, where the transmissions of LoRa Class A devices are affected by path-loss, shadowing and Rayleigh fading. Due to the possibility of capturing multiple frames simultaneously, we consider the maximum achievable performance of the PHY/MAC LoRa scheme according to the Signal-to-interference-plus-noise ratio. The contribution of this work is primarily focused on studying the average number of successfully received LoRa frames, which constitutes a performance upper bound due to the optimal capture condition considered in the PHY-layer. We show the impact of path loss and fading effects on the average number of successfully received frames for different levels of network traffic load. Numerical and simulation results are used to evaluate the accuracy of the performance model, showing that it can be effectively used to anticipate an upper-bound of the performance when PHY-layer conditions are known in advance. The upper-bound is due to the fact that current LoRa receivers are unable to decode multiple frames at the same time. However, the results presented in the paper clearly show the advantages of adopting receivers capable of decoding multiple frames simultaneously, which can effectively increase the capacity of future LoRa devices.

References

[1] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, Secondquarter. 2017.

[2] TheThingsNetwork. Accessed Jan., 2019. [Online]. Available: https://www.thethingsnetwork.org

[3] Semtech. LoRa Modulation Basics. Accessed Jan., 2019. [Online]. Available: https://www.semtech.com

[4] LoRaWAN. LoRa Alliance. Accessed Jan., 2019. [Online]. Available: https://lora-alliance.org

[5] P. Neumann, J. Montavont, and T. Noël, "Indoor deployment of low-power wide area networks (LPWAN): A LoRaWAN case study," in *Proc. IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Commun. (WiMob)*, New York, NY, USA, Oct. 2016, pp. 1–8.

[6] O. Iova, A. L. Murphy, G. P. Picco, L. Ghiro, D. Molteni, F. Ossi, and F. Cagnacci, "LoRa from the City to the Mountains: Exploration of Hardware and Environmental Factors," in *Proc. of the Int. Conf. on Embedded Wireless Systems and Networks*, 2017, pp. 317–322.

[7] A. Rahmadhani and F. Kuipers, "When lorawan frames collide," in *Proceedings of the 12th International Workshop on Wireless Network Testbeds, Experimental Evaluation; Characterization*, ser. WiNTECH '18. New York, NY, USA: ACM, 2018, pp. 89–97. [Online]. Available: http://doi.acm.org/10.1145/3267204.3267212

[8] C. Goursaud and J.-M. Gorce, "Dedicated networks for iot : Phy / mac state of the art and challenges," in *EAI endorsed transactions on Internet of Things, European Alliance for Innovation,*, 2015.

[9] M. C. Bor, U. Roedig, T. Voigt, and J. M. Alonso, "Do lora low-power wide-area networks scale?" in *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, ser. MSWiM '16. New York, NY, USA: ACM, 2016, pp. 59–67. [Online]. Available: http://doi.acm.org/10.1145/2988287.2989163

[10] O. Georgiou and U. Raza, "Low Power Wide Area Network Analysis: Can LoRa Scale?" *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 162–165, Apr. 2017.

[11] A. Waret, M. Kaneko, A. Guitton, and N. E. Rachkidy, "LoRa Throughput Analysis with Imperfect Spreading Factor Orthogonality," *IEEE Wireless Commun. Lett.*, 2018.

[12] G. Nguyen, A. Ephremides, and J. Wieselthier, "On capture in random-access systems," *IEEE Int. Symp. on Information Theory*, Jul. 2006.

[13] A. Abdi and M. Kaveh, "On the utility of Gamma PDF in modeling shadow fading (slow fading)," in *Proc. IEEE Veh. Technol. Conf.*, Houston, TX, USA, May 1999, pp. 2308–2312.

[14] D. Lewinski, "Nonstationary probabilistic target and clutter scattering models," *IEEE Trans. Antennas Propag.*, vol. 31, no. 3, pp. 490–498, May 1983.

[15] S. Al-Ahmadi and H. Yanikomeroglu, "On the approximation of the Generalized-K distribution by a Gamma distribution for modeling composite fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 706–713, Feb. 2010.

[16] Semtech. Application note an1200.22, lora modulation basics. Accessed Jan., 2019. [Online]. Available: https://www.semtech.com/uploads/documents/an1200.22.pdf

[17] A. Furtado, R. Oliveira, R. Dinis, and L. Bernardo, "Successful packet reception analysis in multi-packet reception wireless systems," *IEEE Communications Letters*, vol. 20, no. 12, pp. 2498–2501, Dec 2016.

[18] F. W. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, *NIST Handbook of Mathematical Functions*, 1st ed. New York, NY, USA: Cambridge University Press, 2010.

[19] Semtech. SX1272/73 - 860 MHz to 1020 MHz Low Power Long Range Transceiver, Datasheet. Accessed Jan., 2019. [Online]. Available: https://www.semtech.com/uploads/documents/sx1272.pdf